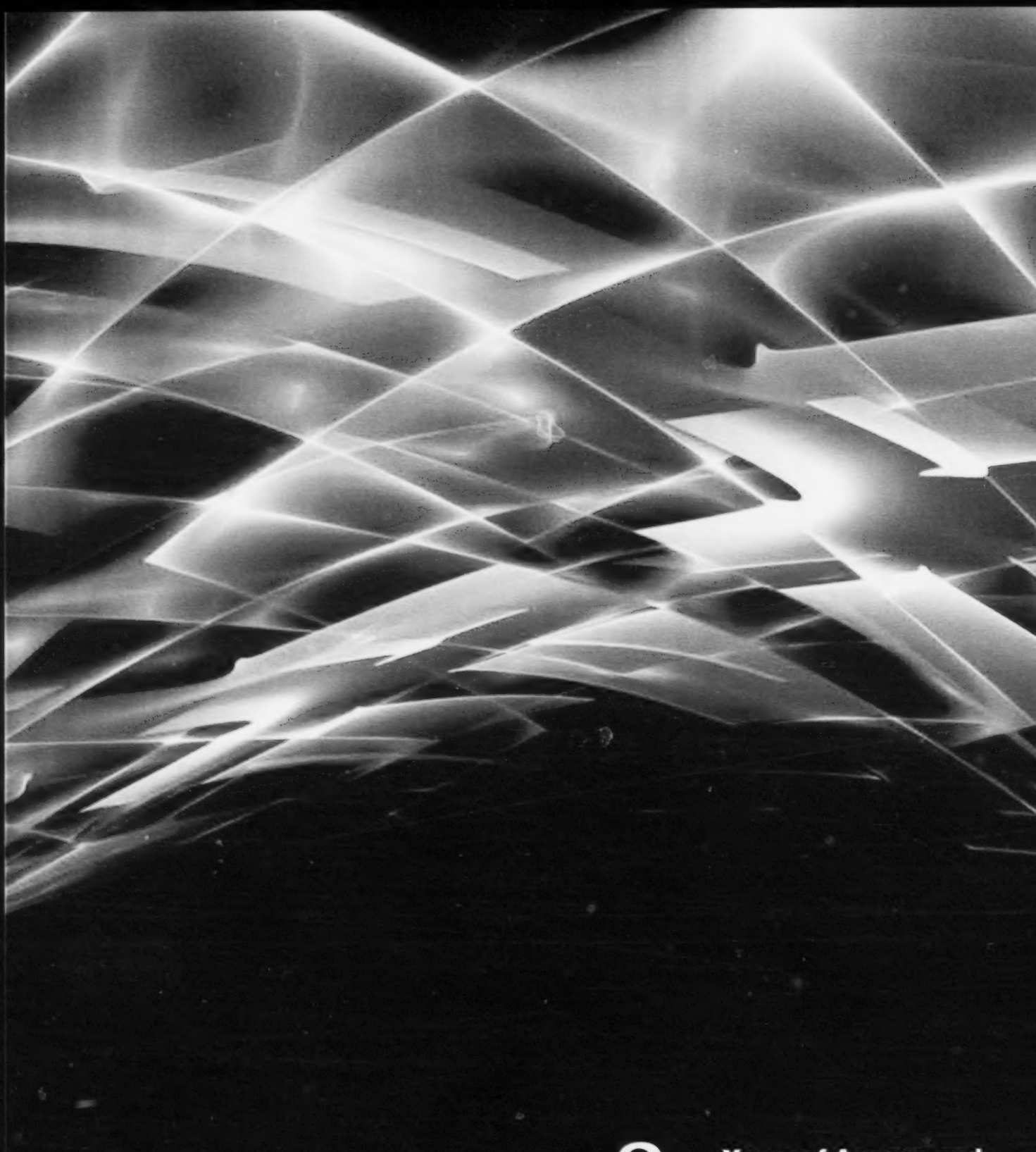


25 Years of Access and Privacy Leadership

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER, ONTARIO, CANADA

25 YEARS OF ACCESS AND PRIVACY LEADERSHIP

Commissioner's Message

2012 MARKED THE 25TH ANNIVERSARY OF THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER (IPC) FIRST OPENING ITS DOORS IN LATE 1987, as a handful of newly hired staff prepared for the *Freedom of Information and Protection of Privacy Act* coming into effect on January 1, 1988. I was lucky to be among the first who served on Justice Sidney B. Linden's startup team. I still find it hard to believe that a quarter-century has passed since I joined the IPC as the office's first Director of Compliance, then Assistant Commissioner. For the last fifteen years, I have had the honour of serving as its Commissioner.

During that time, I have also been fortunate to find myself in a unique historical position as the advent of the Internet and the Web drastically changed the very concept of how we view access and privacy. Never before in our history has information been so readily available – for better and for worse. The information technology revolution of the mid-1990s brought with it a myriad of advances with enormous benefits to society, such as greater access to information. It also gave birth to an entire new paradigm of concerns regarding privacy and the protection of personal information. Advances in information technology have not only inspired people to develop new products and services that enhance our everyday lives, they have also given rise to a backlash by those who fear a culture of openness, and further emboldened those who wish to erode our privacy.

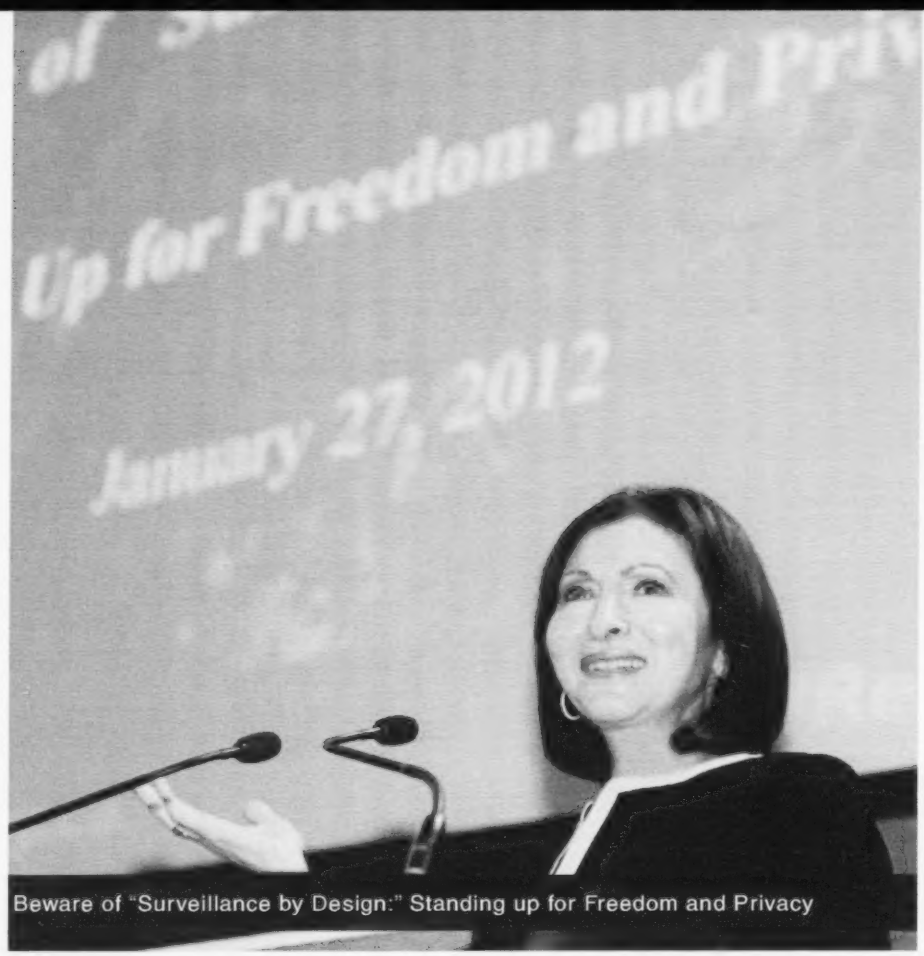
In a perfect world, we would not need the IPC. However, we do not live in a perfect world, and despite the great advances we have made in access and privacy, I firmly believe that our efforts are needed now more than ever. That is why the theme of this year's Annual Report is "Leadership." As I look back on the last 25 years of the IPC, I believe Ontarians can be assured that this office has grown into a first-class agency known for demonstrating innovation and leadership, in the fields of both access and privacy.

Privacy by Design in 2012

Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities – Win-Win, Toronto Board of Trade

I declared 2011 to be the "Year of the Engineer" as I felt strongly that it was time to reach out to those who actually designed and built the systems and technologies upon which we increasingly rely. I spent much of 2011 bringing *Privacy by Design* (*PbD*) to engineers and software designers, in an effort to operationalize *PbD* at the world's most innovative tech firms. And to my delight, *PbD* was welcomed with open arms! As the New Year began, I felt the need to

reach out even further to call upon innovators and inventors, in order to enlist the support of technology to protect our privacy as opposed to eroding it. And, this lead me to call 2012, the "Year of the Innovator."



Beware of "Surveillance by Design:" Standing up for Freedom and Privacy

Due to the increasingly complex and extrapolative growth of technological advances and the privacy challenges associated with them, we will need innovators to create the solutions we require to protect our privacy, now and well into the future. I found myself spending much of 2012 fighting a common misconception – that privacy stifles innovation. Even today, many perceive privacy to be an impediment, standing in the way of innovation and other goals. Some believe, for example, that security can only be achieved at the expense of privacy, and vice versa – classic zero-sum thinking. On the contrary, I need only to point to *PbD* which has stimulated innovative solutions in privacy protection across a wide spectrum of industries, ranging from biometrics, to health care, to energy.

In addition, more organizations than ever before operationalized the *7 Foundational Principles of PbD* in 2012, which also helped to challenge the myth that privacy stifles innovation. We need only use our imaginations, abandon zero-sum thinking and embrace positive-sum paradigms. We must replace the "vs." with an "and" thus allowing for win-win solutions for the future of privacy, and indeed, paving the way for the future of freedom.

For a number of years, I have worked steadily to transform *PbD* from a concept into a world-renowned framework. Last year, the popular American political blog *Politico* wrote, "Washington is obsessed with the concept of '*Privacy by Design*' — it's in the FTC's privacy report and it guides the White House's online privacy blueprint." While I am very proud that *PbD* has spread internationally, I also wanted to ensure that it was strongly adopted here in Ontario, where as you know, it was created. That is why I am teaming up with the Ontario Public Service to create a *Privacy by Design Centre of Excellence* to be launched in early 2013. My intention is to have the *PbD Centre of Excellence* provide leadership and best practices, as well as to ensure that privacy is embedded as the default condition, in both new and existing government programs. The opportunities for implementation are endless. The formal adoption of *PbD* across all levels of Ontario's government will indeed secure our place as world-class leaders in privacy and data protection.

Beware of "Surveillance by Design:" Standing Up for Freedom and Privacy - Nathalie Des Rosiers, General Counsel, Canadian Civil Liberties Association; Dr. Ann Cavoukian, Information and Privacy Commissioner, Ontario; John Ibbitson, Ottawa Bureau Chief, the Globe and Mail

In May, my office, in association with University of Toronto's Identity, Privacy and Security Institute, which I Chair, presented the first *SmartData* International Symposium at the University of Toronto. The symposium was host to over two dozen international, multi-disciplinary experts who spent three days presenting the vision of *SmartData* as the key to ensuring the protection of privacy online, well into the 21st century. The symposium confirmed what I have long believed to be true: that rejecting the widespread, zero-sum perspective that privacy and business objectives must, by necessity, be in conflict, opens up a world of possibilities. One of these possibilities is *SmartData*, which I believe is the strongest possible expression of *PbD* and represents the next generation of *PbD* – or *PbD 2.0*. It advocates that control over one's own personal data should lie with the individual to whom the data pertains, not with an organization. The individual benefits greatly by regaining control over his or her personal information without having to assume the burden of constantly exercising control for each data request. Moreover, unlike many systems which aim to protect data, *SmartData* enables the data to protect itself. By designing privacy directly into the data, it is necessarily designed into all transactions involving that data!

In this era of Big Data, personal information – considered to be the "oil" of the Internet – largely resides with organizations – removed from the individual's sphere of control. The boundless potential of the Personal Data Ecosystem (PDE) is to place control of one's personal information into the hands of the individual. I believe that PDE is truly a game changer, and will move privacy well beyond laws, regulations and best practices, to create a privacy-protective relationship between individuals and organizations. In October, I released a discussion paper entitled, *Privacy by Design and the Emerging Personal Data Ecosystem*, which Politico called a "Hot Doc: One Privacy Paper to Read This Week." The paper describes the systems and initiatives driving the PDE and how they seek to address the challenge of protecting and promoting privacy, while at the same time, encouraging the socio-economic opportunities and benefits of personal information as a new asset class.

Now recognized as an International Standard and translated into 30 languages, *Privacy by Design* has been put into practice by a growing number of organizations worldwide, to make privacy the default setting. However, I felt it was necessary to provide further guidance through this potentially challenging process. In December, I released a new white paper,

Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices, which provides an anthology of real-world experiences, lessons learned and successes encountered in implementing the *PbD* framework from a wide range of sectors including telecommunications, technology, health care, biometrics, sensors, transportation, and energy. The end result of implementing these standards is a significant privacy payoff – a sustainable, business-friendly environment which provides superior protection from data leaks or breaches. This in turn creates a significant competitive advantage. Building privacy into the business ecosystem yields many benefits, ranging from cost-savings, to strengthening business/consumer relationships, to enhancing much-needed trust.

2012 Highlights

In January I held a public symposium called, "Beware of Surveillance by Design: Standing up for Freedom and Privacy," bringing together a highly respected panel of thought leaders to share their perspectives and raise awareness of the serious privacy implications of online surveillance in proposed federal "lawful access" legislation. I was gratified when people from across the political and social spectrum rallied to the defence of privacy in response to the government introducing Bill C-30 and on Valentine's Day, of all days! To its credit, the federal government put the proposed legislation on hold shortly after its introduction in Parliament and the subsequent public storm of concern from Canadians. The key question for 2013 is whether Bill C-30 will be redesigned to incorporate the necessary privacy protections. We learned the answer to that early in 2013, and were absolutely delighted with its demise! ***Note:*** *On February 11, 2013, the federal government announced that it would not proceed with Bill C-30, and any attempts to modernize the Criminal Code will not contain the measures in C-30, including the warrantless mandatory disclosure of basic subscriber information or the requirement for telecommunication service providers to build intercept capability within their systems.*

I was asked by two Members of Provincial Parliament in May to investigate the privacy and security of personal information of people who had applied for hunting and fishing licences. This information is currently being stored in the United States as part of an outsourced Licensing Automation System (LAS) system by

Beware of "Surveillance by Design:" Standing Up for Freedom and Privacy - Dr. Ron Deibert, Professor, Political Science, University of Toronto; Dr. John Villasenor, Non-resident Senior Fellow in Governance Studies, the Brookings Institution and Professor, Electrical Engineering, University of California, Los Angeles

the Ministry of Natural Resources. Specific concerns were raised about the collection and storage of personal information in light of the U.S. PATRIOT Act. I found that the Ministry's collection, use and disclosure of personal information for the purpose of administering the Ministry's hunting and fishing licensing program was in full compliance with Ontario's *Freedom of Information and Protection of Privacy Act*. I made several recommendations for changes to the notices of collection that were previously in use by the Ministry, which they agreed to.

There may be no greater area of confusion and misunderstanding than fear of the PATRIOT Act, which has invoked unprecedented levels of apprehension and consternation. What is not widely known is that the feared powers were already available to law enforcement long before the passage of the PATRIOT Act, through a variety of legal instruments. I believe it is far more productive to compel organizations to be fully responsible and accountable for the services they provide or outsource. I have always said – you can outsource services, but you cannot outsource accountability.

I was deeply disturbed in July when Greg Essensa, the Chief Electoral Officer advised me that staff at Elections Ontario had lost two USB keys containing the unencrypted personal information of up to 2.4 million Ontarians. When Mr. Essensa asked for my assistance in investigating this matter and to advise him on how to prevent another breach from occurring, I of course agreed. Ultimately, at the root of the problems uncovered during my investigation was a failure to build privacy into the routine information management practices of the organization. I recommended concrete steps that Elections Ontario must take to enhance the protection of personal information and restore the trust of Ontarians. I was very pleased that Mr. Essensa accepted my recommendations unreservedly – Elections Ontario has made significant progress in implementing them.

In September, my office hosted an event on the global Open Data movement with the Toronto Board of Trade to mark Right to Know Week, which is celebrated by freedom of information organizations in over 40 countries around the world. I was impressed by the excellent work being done right here by the City of Toronto! I was pleased to learn that the Government of Ontario had heeded the call in my 2011 Annual Report to establish its own Open Data portal. My message to those gathered was that all public institutions in Ontario should take advantage of emerging technologies to make data (general records) available to the public, academics, researchers, and industry, for use in new and unanticipated ways – by default.

Following a series of high profile bullying incidents in 2012, including some with the most tragic of outcomes, I felt the need to again speak out on this issue. I released a special video blog and reached out to junior high school students, speaking to them directly about actual incidences of bullying and its heart-breaking consequences. I urged those who witnessed bullying not to stay silent and to speak up. In November I launched a new initiative, *Stop Bullying... by Design*. The first phase was the creation of a new section on my website with information about online safety, what to do if you become the victim of a bully or if you witness a bullying incident, advice for parents and teachers, and links to important resources. Watch for more to come in 2013.

My Personal Thank You

As always, I would like to give my sincere thanks to all of our IPC staff – past and present. So much has transpired since this office first opened its doors 25 years ago. I have seen the demands and pressures on my office grow significantly, repeatedly exceeding the growing expectations placed upon them. There have been many occasions where I was genuinely touched by the diligence and enthusiasm shown by my staff. I truly believe that the people of Ontario are very fortunate to have such talented and dedicated people working on their behalf, in the pursuit of open, transparent government, and the protection of our personal privacy – at the heart of our freedom and liberty. You are all true professionals. I give you my heartfelt thanks, now and always!

ANN CAVOUKIAN, Ph.D.
INFORMATION & PRIVACY COMMISSIONER, ONTARIO, CANADA

"IN A PERFECT WORLD, WE WOULD NOT NEED THE IPC. HOWEVER, WE DO NOT LIVE IN A PERFECT WORLD, AND DESPITE THE GREAT ADVANCES WE HAVE MADE IN ACCESS AND PRIVACY, I FIRMLY BELIEVE THAT OUR EFFORTS ARE NEEDED NOW MORE THAN EVER."

ANN CAVOUKIAN, Ph.D.

Ontario's Information and Privacy Commissioners: Honourable Sidney B. Linden (1987 – 1991), Dr. Ann Cavoukian (1997-Present), Tom Wright (1991 – 1997)

25 YEARS OF ACCESS AND PRIVACY LEADERSHIP TWO THOUSAND AND TWELVE

Table of Contents

Commissioner's Message	1
Commissioner's Recommendations	13
Privacy by Design: Year in Review	18
Lawful Access	24
IPC Anniversary Timeline	Centrefold
Key Issues	30
Access	38
PHIPA in 2012	48
Judicial Reviews	51
Financial Statement	IBC

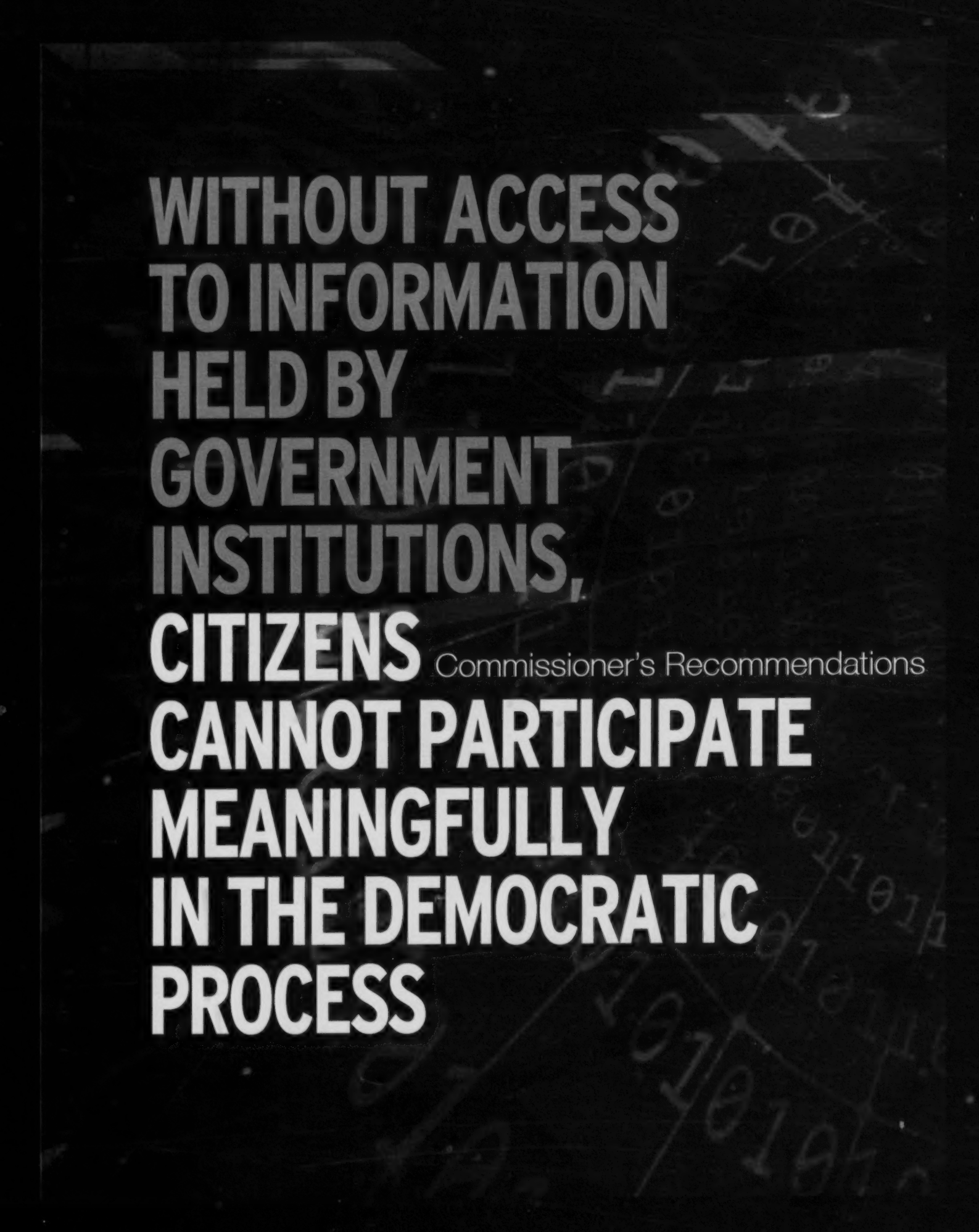
WE DO NOT LIVE IN A PERFECT WORLD,
AND DESPITE THE GREAT ADVANCES WE HAVE MADE IN ACCESS AND PRIVACY, I FIRMLY BELIEVE THAT OUR EFFORTS ARE NEEDED NOW MORE THAN EVER. THAT IS WHY THE THEME OF THIS YEAR'S ANNUAL REPORT IS

LEADE

RSHIP

AS I LOOK BACK

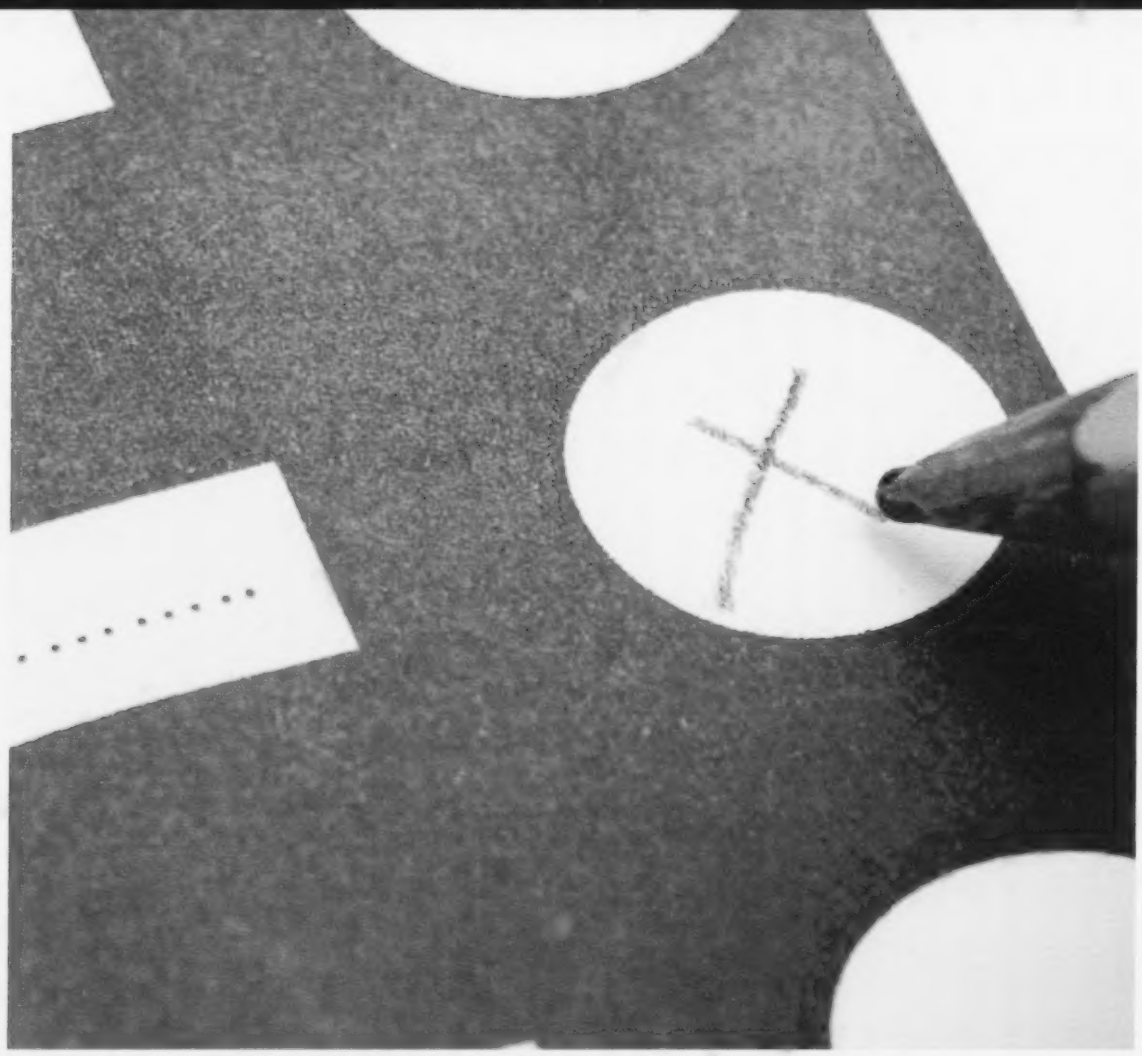
ON THE LAST 25 YEARS OF THE IPC, ONTARIANS CAN BE ASSURED THAT THIS OFFICE HAS GROWN INTO A FIRST-CLASS AGENCY KNOWN FOR DEMONSTRATING INNOVATION AND LEADERSHIP IN THE FIELDS OF BOTH ACCESS AND PRIVACY.


WITHOUT ACCESS
TO INFORMATION
HELD BY
GOVERNMENT
INSTITUTIONS,
CITIZENS
Commissioner's Recommendations
CANNOT PARTICIPATE
MEANINGFULLY
IN THE DEMOCRATIC
PROCESS

Children's Aid Societies

One of the foundational tenets of freedom of information is that organizations that receive significant public funding should be subject to public scrutiny through freedom of information laws. Ontario has made important advances in this effort by extending the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) to universities in 2006 and hospitals in 2012, but there are still institutions in the government and Broader Public Sector which are not covered by the *Acts*.

I recommend that the government launch a comprehensive review to compile a list of institutions, including Children's Aid Societies, which are primarily funded by government but are not yet covered by *FIPPA* or *MFIPPA*, the *Municipal Freedom of Information and Protection of Privacy Act*. This should be followed by a prompt assessment of these institutions – with the default position being that each institution on the list will be added to the appropriate *Act*, unless there are compelling reasons not to add a specific institution.



Election Act

Two fundamental concerns with regard to the *Election Act* arise from my office's investigation into a privacy breach at Elections Ontario. First, the information lost includes electors' personal information that is only available to political parties and MPPs through the Permanent Register of Electors for Ontario, and is to be used for electoral purposes only. This information is not available to the general public in any form. Second, the information lost was in electronic format which heightens concerns for its misuse, given the realities of the digital age.

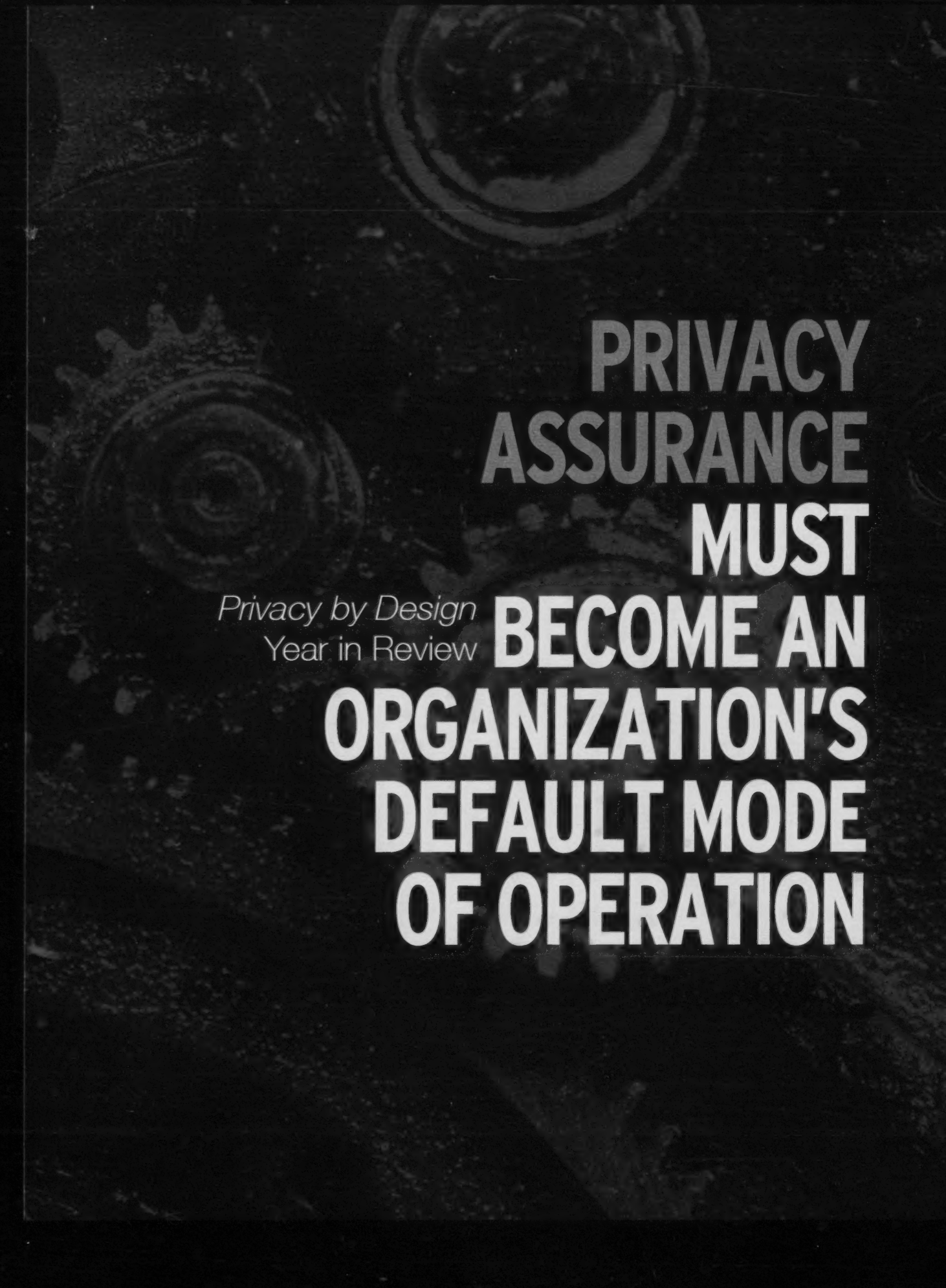
I therefore recommend that the Ontario government review the provisions of the *Election Act* to consider what changes need to be made to ensure that only necessary elector information is collected, and appropriate protections and oversight are in place to protect against improper uses of voter information, by both individuals and political parties, and to ensure that the personal information of electors is secured throughout the entire lifecycle of the data.

Privacy by Design in the Ontario Public Service

The irony of a privacy breach, such as the one at Elections Ontario, occurring in our province is the fact that *Privacy by Design* – unanimously passed as an International Privacy Standard in 2010, originated in Ontario. *Privacy by Design* is now being followed all around the world and has been recommended repeatedly by the Federal Trade Commission in the United States and is referenced several times in the European Union's draft Data Protection Regulation.

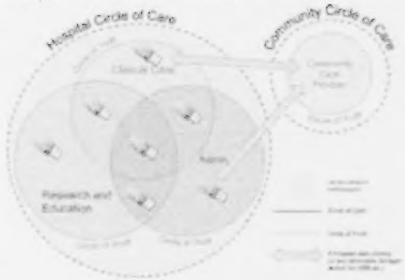
While *Privacy by Design* is being implemented in parts of the Ontario Public Service, and the first steps are being taken in the creation of a joint *Privacy by Design* Centre of Excellence with my office and the OPS, there is still much work to be done.

To ensure strong privacy protections are embedded in all sectors of the government, I urge the government of Ontario to mandate that a *Privacy by Design* approach be taken for all new information technologies, business practices, networked infrastructures, and physical designs in the Ontario Public Service and Broader Public Sector.


PRIVACY ASSURANCE MUST BECOME AN ORGANIZATION'S DEFAULT MODE OF OPERATION
Privacy by Design
Year in Review

Encryption by Default and Circles of Trust: Strategies to Secure Personal Information in High-Availability Environments

As portable storage devices become increasingly prevalent in the health-care sector, concerns also arise regarding the privacy and security of personal health information (PHI), which can be offset by the use of encryption as the default.



Operationalizing *Privacy by Design*: A Guide to Implementing Strong Privacy Practices

The international standard of *Privacy by Design* can be leveraged as an actionable framework and is currently in use with partners and in projects around the world.

Abandon Zero-Sum, Simplistic either/or Solutions – Positive-Sum is Paramount: Achieving Public Safety and Privacy

Privacy by Design provides a win-win solution for surveillance programs and associated technologies when applied in a positive-sum manner, allowing public safety initiatives and privacy protection to coexist.

Operationalizing *Privacy by Design*

Privacy by Design (*PbD*) has achieved significant recognition over the years and with increased understanding and adoption came new questions about how to implement such a framework. To address these concerns, we created a new document that would act as a compendium – consolidating real-world examples of individuals and organizations that have been operationalizing *Privacy by Design* and illustrating how they have been benefitting from this for over a decade.

The document, published this past December, is titled, "Operationalizing *Privacy by Design*: A Guide to Implementing Strong Privacy Practices." In the document, I provided an anthology of real-world experiences from organizations across a wide range of sectors including telecommunications, technology, health care, transportation, and energy. In fact, there are an endless number of areas where *PbD* might be operationalized, but much of our *PbD* research is directly related to one of nine key application areas:

1. CCTV/Surveillance Cameras in Mass Transit Systems;
2. Biometrics Used in Casinos and Gaming Facilities;
3. Smart Meters and the Smart Grid;
4. Mobile Devices & Communications;
5. Near Field Communications (NFC);
6. RFIDs and Sensor Technologies;
7. Redesigning IP Geolocation Data;
8. Remote Home Health Care;
9. Big Data and Data Analytics.

Furthermore, if an organization is to properly operationalize *PbD*, then it must engage all levels of the organizational hierarchy. In other words, it is not only executives who must get involved, but software engineers and designers, risk managers, marketing and customer service professionals, legal departments, project managers, privacy

officers, and likely many others as well. In addition, if we are to engage the entire organization, we must be sure to incorporate the associated business requirements, engineering specifications, development methodologies, and security controls, according to each domain or project scope.

There are many organizations that are operationalizing *Privacy by Design* right now and it is my hope that as they do so, they will make their own stories available so that the privacy community may continue to build much-needed expertise and grow best practices for the benefit of all. I can humbly admit that our work is far from complete – in fact, it has just begun. However, I hope that our achievements in these areas will serve as an example to other individuals and organizations that operationalizing *Privacy by Design* is not only possible, but enormously valuable.

SmartData Symposium

In this era of Big Data, online information is increasing at a rate that is virtually incomprehensible to the average human being. As a result, we will need to find innovative ways to allow individuals to protect their personal information. However, we are constantly presented with the scenario that we have to choose between privacy *or* sharing; between privacy *or* public safety. This is a false zero-sum paradigm that does not take into account the power of human ingenuity to create a positive-sum solution that delivers both privacy *and* sharing; privacy *and* public safety.

SmartData is a concept that represents the embodiment of *Privacy by Design* (*PbD*), placing the user firmly in the driver's seat. In fact, one might consider SmartData to be the next evolution of *Privacy by Design* – *PbD 2.0*.

Privacy by Design and User Interfaces: Emerging Design Criteria – Keep it User-Centric

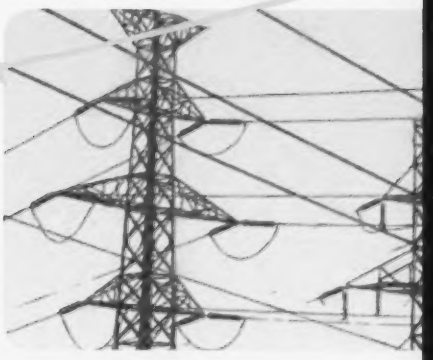
User-centric design principles allow for a customized online experience where the user is able to express their own privacy preferences.

Building Privacy into Ontario's Smart Meter Data Management System: A Control Framework

The *Privacy by Design* framework is being applied by Ontario's Smart Metering Entity in support of the province's Smart Metering Initiative.

Privacy by Design in the Age of Big Data

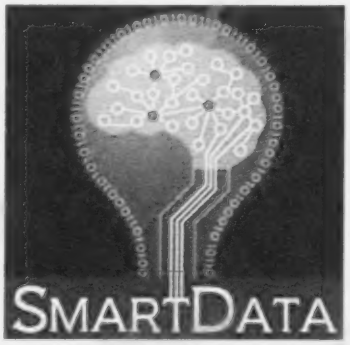
Big Data and privacy successfully coexist within this "sensemaking" (a term coined by Jeff Jonas, IBM Fellow, Chief Scientist, IBM Analytics) technology that was engineered, from the ground up, with privacy-enhancing features.

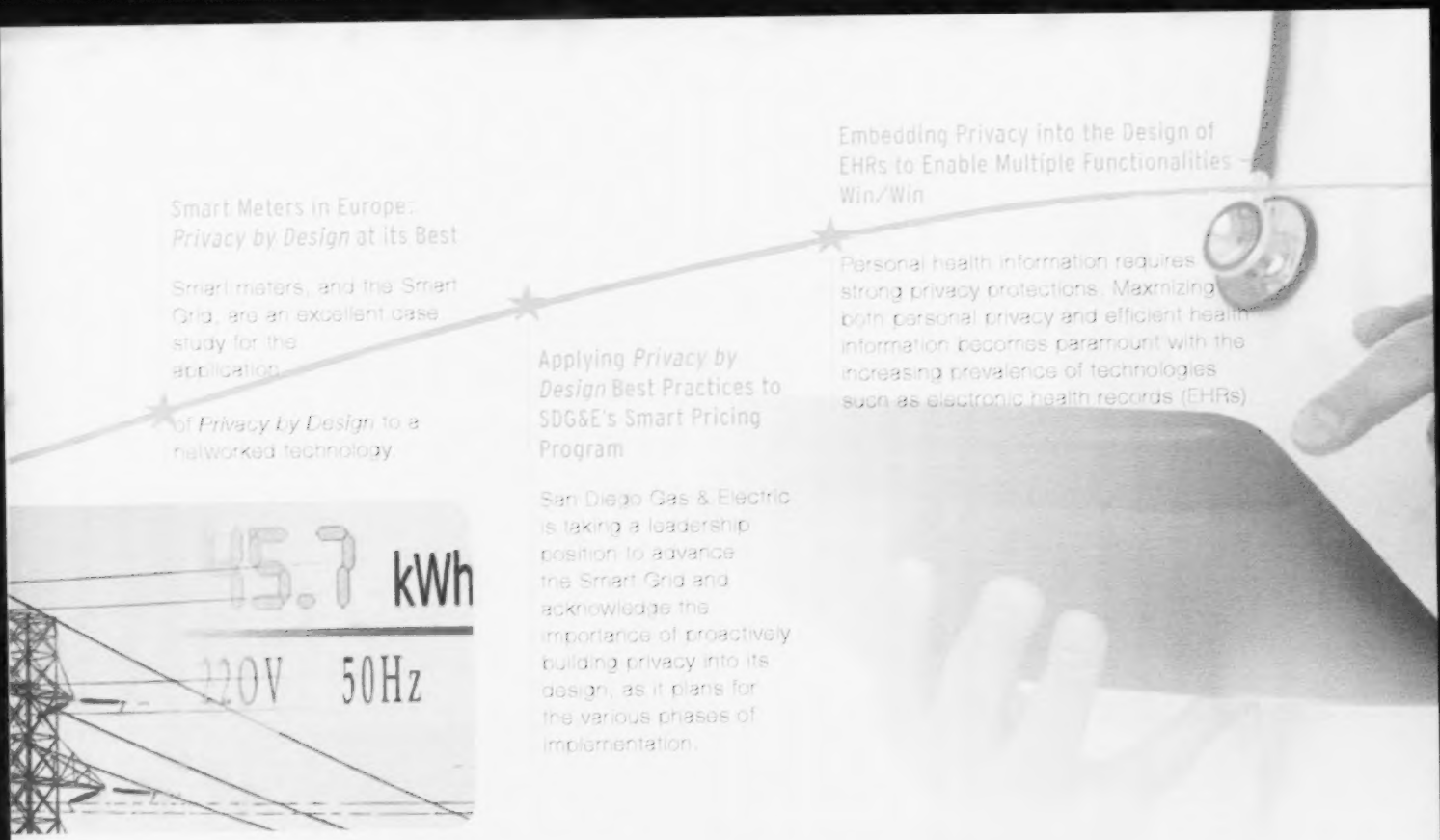


SmartData aims to provide a positive-sum solution by creating Internet-based virtual agents which will act as an individual's online proxy to securely store his or her personal information, and disclose it based upon the context of the data request and instructions authorized by the data subject. In other words, the individual, via his/her intelligent agent on the Web, would be in complete control of his/her personal information at all times. No longer could organizations use personal data in ways that contradicted an individual's choices (unless authorized by a judicial warrant).

To launch this initiative, my office held a Symposium jointly with the University of Toronto from May 14-16. The *SmartData International Symposium* was co-hosted by the Identity, Privacy & Security Institute (IPSI) and featured some of the world's foremost experts in robotics, privacy, artificial intelligence, cognitive science, computer science, evolutionary biology, engineering, and philosophy. It is also important to note that in keeping with the University of Toronto's rich research history, principal funding for this Symposium was provided by the University of Toronto's Connaught Fund.

The implementation of SmartData represents a quantum leap in people's ability to control the collection, use, and disclosure of their personal information. The development of SmartData will return personal privacy – the basis of our freedom and liberty – back to the individual, where it belongs.




Smart Meters in Europe: *Privacy by Design* at its Best
Smart meters, and the Smart Grid, are an excellent case study for the application
of *Privacy by Design* to a networked technology.
Applying *Privacy by Design* Best Practices to SDG&E's Smart Pricing Program
San Diego Gas & Electric is taking a leadership position to advance the Smart Grid and acknowledge the importance of proactively building privacy into its design, as it plans for the various phases of implementation.
Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities – Win/Win
Personal health information requires strong privacy protections. Maxmizing both personal privacy and efficient health information becomes paramount with the increasing prevalence of technologies such as electronic health records (EHRs).
45.7 kWh
220V 50Hz

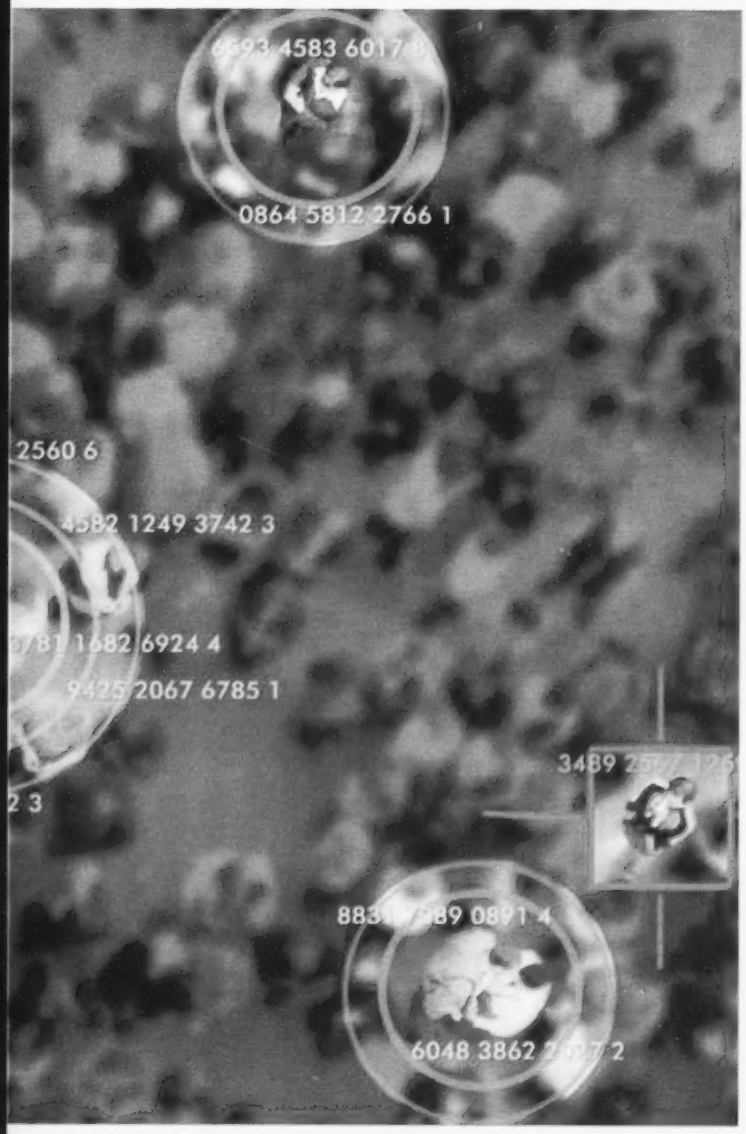
Privacy by ReDesign – University of Toronto Projects

One of my least favourite myths about privacy is that "privacy is dead" and it is compounded when it is attributed to new technological innovations or to a changing mindset amongst young people. If you ever doubted the existence of privacy-conscious students, look no further than the Identity, Privacy and Security Institute (IPSI) at the University of Toronto. IPSI aims to deliver an interdisciplinary program that tackles research, education, outreach, and industry collaboration – and it is there that you will find an incredibly intelligent group of privacy-conscious innovators and thought leaders.

In late December, I was invited as an honorary guest to review a group of student projects. The students were part of a Master's Program that incorporates the Department of Electrical and Computer Engineering as well as the Faculty of Information. The students were tasked with finding new and innovative ways to embed privacy into legacy systems. With the future in mind, the students developed ingenious methods of redesigning both the policies and the technologies of modern-day products and services to incorporate strong privacy settings. The projects addressed several areas where privacy could be improved, such as popular gaming systems, as well as Web and mobile applications. The results were outstanding! There were numerous concrete examples of *Privacy by ReDesign* (*PbRD*) and – without exaggeration – all of the projects were brilliant. I am confident that we will see more innovative ideas for redesign as an increasing number of students get involved and change the way we think about privacy.

TOGETHER WE DEMONSTRATED THAT THE TRUE VALUE OF PRIVACY MUST BE RECOGNIZED

Lawful Access



UNLAWFUL ACCESS

This past year was extremely significant in the battle to ensure that Canadians' privacy rights are fully respected, as Parliament considered the federal government's latest proposal for new online surveillance legislation. My office was in the forefront of that battle.

I began the year by launching RealPrivacy.ca to draw attention to potential dangers of such legislation. To coincide with International Privacy Day, I hosted a public symposium, entitled "Beware of Surveillance by Design: Standing Up for Freedom and Privacy." The goal of both the website and the symposium was to raise awareness of the serious privacy implications of online surveillance and the then imminent return of the proposed legislation. Speakers at the symposium included highly-respected thought leaders in privacy, technology and the law, a prominent journalist, and civil liberties leaders. This standing-room-only event attracted public safety and law enforcement officials, elected representatives, individuals from the telecoms, as well as members of the general public. It helped to mobilize and expand an informed public discussion about the Government's proposed surveillance bid.

Commissioner Cavoukian spoke publicly and to the media numerous times to educate highlights of the campaign against surveillance by design.

OCT 31, 2011 NOV 28, 2011 DEC 14, 2011 JAN 12, 2012 JAN 25, 2012 JAN 25, 2012

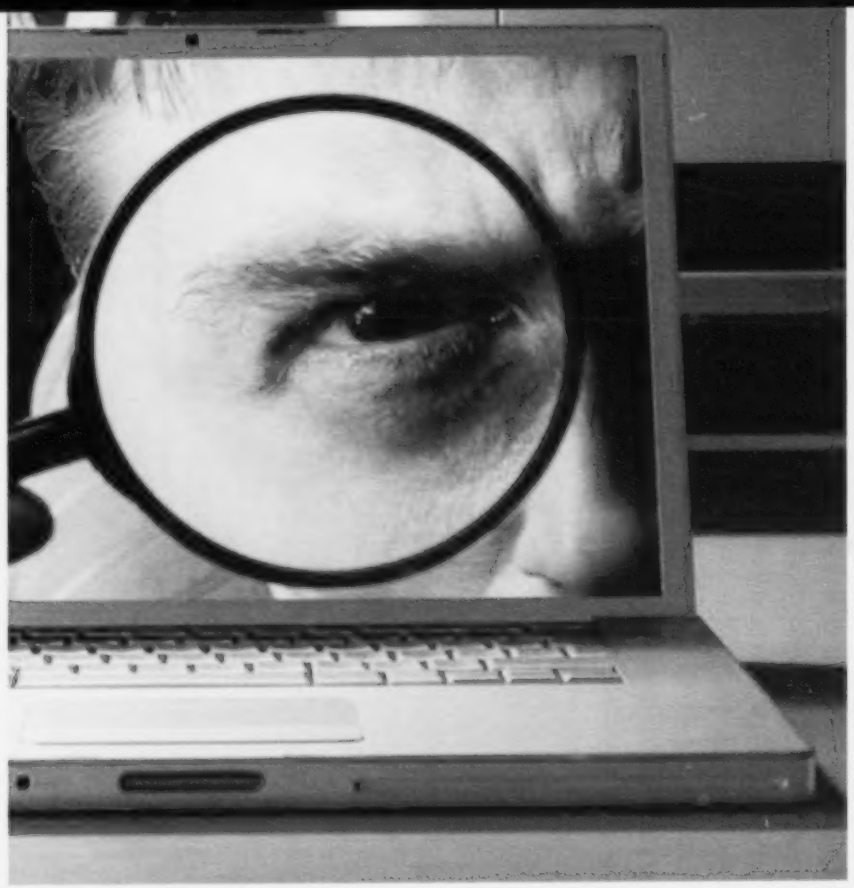
In the days leading up to the symposium, my office also created a Web-based campaign, inviting Canadians to email their members of Parliament to ask them to champion freedom and privacy. We provided information and resources to help ensure that citizens and elected officials understood the critical privacy issues.

I was gratified when people from across the political and social spectrum rallied to the defence of privacy when the government introduced Bill C-30 on February 14th – Valentine's Day! To its credit, the government put the proposed legislation on hold shortly after its introduction in Parliament and the subsequent storm of concern from Canadians.

As I indicated in my last Annual Report, such a proposal represents a looming system of warrantless "Surveillance by Design" that

the public about the dangers of unlawful access. This timeline marks some of the

JAN 27, 2012 FEB 14, 2012 FEB 14, 2012 FEB 14, 2012 FEB 15, 2012 FEB 16, 2012



should concern us all in a free and democratic society. Just consider, that if passed without significant amendments, the bill's warrantless subscriber data provisions would provide police with a much greater ability to access and track information about identifiable individuals via the communications technologies that we use every day, such as the Internet, smart phones, and other mobile devices, and at times, without a warrant or any judicial authorization.

Properly supervised, surveillance powers can be invaluable to law enforcement. However, it is equally true that where individuals are subject to unwarranted suspicions, evidence is poorly handled, or erroneous conclusions are hastily drawn, the consequences for innocent individuals and our fundamental freedoms can be devastating. That is why we have worked so hard to identify and propose positive-sum solutions so that Canadians can have both effective law enforcement and robust privacy protection.

Throughout 2012, I worked to ensure that our privacy concerns remained front and centre in this debate. I spoke with major media across Canada, on numerous occasions, to raise awareness and draw attention to our strong concerns with this legislation. I incorporated these concerns into a number of speeches that I delivered to diverse audiences such as the Canadian Bar Association and Senaca College. In the spring, I wrote to law enforcement officials and the responsible Federal minister with concrete recommendations to assist in the necessary redrafting of Bill C-30. In the fall, alongside my colleagues, B.C. Information and Privacy Commissioner Elizabeth Denham and Alberta Information and Privacy Commissioner Jill Clayton, I participated in a spirited exchange

FEB 18, 2012 FEB 18, 2012 FEB 22, 2012 FEB 23, 2012 APR 4, 2012 MAY 14, 2012

through the media with representatives of the Canadian Association of Chiefs of Police over the privacy implications of Bill C-30. As the year drew to a close, I recommitted to my goal of advocating for privacy-protective amendments.

As we move through this 25th year of access and privacy legislation in Ontario, my office will stay vigilant in our efforts to protect the online privacy of Ontarians and Canadians. We can, and must, have both security *and* privacy, in unison. It should not be one at the expense of the other. The true value of privacy must be recognized – and ideally enhanced, not diminished – in any effort to modernize law enforcement powers.

Note: *On February 13, 2013, federal Justice Minister Rob Nicholson announced that the Government would not be proceeding with Bill C-30. I'm delighted that the Government listened to the enormous public outcry against unauthorized, warrantless access. I want to express my sincere thanks to Ontarians, and indeed all Canadians, who joined us by the thousands in standing up for freedom and democracy. Together we demonstrated that the true value of privacy must be preserved, not weakened, in efforts to modernize law enforcement powers.*

Commissioner Cavoukian addresses the Toronto Board of Trade

MAY 23, 2012 JUN 25, 2012 SEP 5, 2012 NOV 7, 2012 NOV 14, 2012 DEC 6, 2012

25 YEARS OF ACCESS AND PRIVACY LEADERSHIP

IPC Anniversary Timeline

1987

Ontario's *Freedom of Information and Protection of Privacy Act* (*FIPPA*) passes

The *Act* passes Third Reading on June 25, and receives Royal Assent on June 29, 1987.

Justice Sydney B. Linden appointed as first Commissioner

Justice Linden becomes the first Information and Privacy Commissioner for Ontario, leading a small team in establishing the new agency's role and developing jurisprudence.

1988

***The Freedom of Information and Protection of Privacy Act* comes into force January 1, 1988**

The *Act*, which gives individuals the right to request access to government-held information, including general records and records containing their own personal information, and requires that the government protect the privacy of an individual's personal information held in government records, comes into effect.

1991

***Health Cards and Numbers Control Act* is passed**

This legislation is enacted after the IPC stresses to the government the need for such a law (in this case, to control the use of the new provincial health numbers in both the public and private sectors).

Tom Wright succeeds Justice Linden as Commissioner

After serving for nearly three years, Justice Linden is succeeded by Tom Wright. Mr. Wright, who served as the Assistant Commissioner (Access), is appointed as Ontario's second Information and Privacy Commissioner.

***Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) comes into force January 1, 1991**

The municipal *Act* gives individuals the right to request access to information held by local government organizations, including general records and records containing their own personal information, and it requires that these organizations protect the privacy of the personal information they hold. It covers local government organizations, including municipalities, police services and school boards.

1994

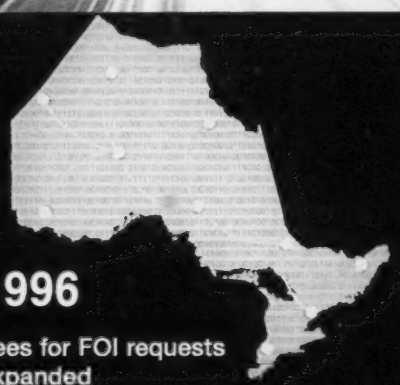
IPC proposes changes to *FIPPA* and *MFIPPA* in a submission to the Standing Committee in the Legislative Assembly

These recommendations are made as part of a three-year review of the municipal *Act*. The IPC calls on the government to extend both access and privacy laws to a wider set of public organizations in order to make important public bodies such as hospitals, universities and social services agencies more accountable to the public.

1995

Privacy-Enhancing Technologies: The Path to Anonymity is published

This groundbreaking paper looks at how technology can be used to help protect privacy. A joint study examines leading technologies that allow anonymous but authenticated transactions – such as blind digital signatures, digital pseudonyms, and the use of trusted third parties.



1996

Fees for FOI requests expanded

The *Savings and Restructuring Act* further amends *FIPPA* and *MFIPPA*, bringing in additional fees. As well, a number of procedural processes are changed and government organizations are given the authority to refuse access in certain circumstances to records on the basis that a request was frivolous or vexatious.

1997

Ann Cavoukian, Ph.D. succeeds Tom Wright as Commissioner

Dr. Ann Cavoukian, who served as the IPC's first Director of Compliance, then as Assistant Commissioner (Privacy), is appointed as Ontario's third Information and Privacy Commissioner.

1998

Drivers maintain their anonymity on Highway 407

The IPC works with the Ontario Transportation Capital Corporation to ensure that the users of the new major electronic toll road, Highway 407, have the option of anonymity (setting up an anonymous prepaid payment account and obtaining a transponder linked to that anonymous account).

Ministry of Education adds freedom of information and protection of privacy to its curriculum for Grade 10 Civics program

The IPC is successful in having access and privacy not only added to the Civics curriculum, but placed in the "Specific Expectations" of what students will learn by the end of the course. Every student in Ontario will learn about the significance of freedom of information and protection of privacy.

2000

***Province of Ontario Savings Office – A Special Report to the Legislative Assembly of Ontario on the Disclosure of Personal Information* is released**

Commissioner Cavoukian tables a special report in the legislature based on an investigation by the IPC into an incident involving account holders of the Province of Ontario Savings Office (POSO). In a special addendum, the Commissioner is very critical of the Ministry of Finance, the ministry responsible for POSO, sparking an emergency debate in the legislature that lasts several days. This is the first – and only – time the Commissioner has to raise such concerns.

2001

Impact on privac after the 9/11 attacks reviewed

Commissioner Cavoukian repeate raises her concern about the new fed *Anti-Terrorism Act*, part of the Canadi government's response to the terrorists' attacks in New York and Washington on September 11, 20 and publishes the essay *Public safet is paramount – bu balanced against privacy*.

2002

IPC proposes open meetings law for municipalities and other public bodies

Commissioner Cavoukian calls on the government to respond to the public's expectation of greater openness and transparency in decision-making by municipalities and other public bodies through the passage of an open meetings law. Key elements of the new law would be: the requirement that public bodies ensure that meetings are open to the public and that proper notice be given; a right for the public to complain if they feel that the rules have not been followed; an oversight body to investigate complaints and resolve disputes; and specific remedies and penalties if the law has been breached. Amendments to the *Municipal Act* and *City of Toronto Act* that brought in open meeting rules for Toronto come into effect on January 1, 2008.

2003

Hydro One and Ontario Power Generation brought under *FIPPA*

After strong encouragement from the IPC, Hydro One and Ontario Power Generation are brought under *FIPPA* by the government. Previously the government divided Ontario Hydro (which was subject to *FIPPA*) into two large companies and several small ones. The two large companies – Hydro One and Ontario Power Generation – were left outside of *FIPPA* at that time.

IPC releases major report: *What to do if a privacy breach occurs: Guidelines for government organizations*

These guidelines are published to assist government institutions, but are applicable by all organizations. They provide guidance on how to identify and contain a privacy breach, whom to notify, and proactive steps to avoid future breaches.

2004

Commissioner Ann Cavoukian, is reappointed

Commissioner Cavoukian is reappointed to a second term as Information and Privacy Commissioner of Ontario. She states her commitment to personal health information in Ontario, as well as to openness and transparency within government.

Release of *Blueprint for Action*

In the *Blueprint for Action*, contained in her Annual Report, the Commissioner makes a series of recommendations designed to promote open, transparent government and the protection of individual privacy in Ontario. In response, within hours of the release of this Annual Report, Premier Dalton McGuinty issues a memorandum to all ministers and deputy ministers calling upon them, "to strive to provide a more open and transparent government."

2005

Adoption Information Disclosure Act is passed

Commissioner Cavoukian strongly urges the government to amend its proposed *Adoption Information Disclosure Act*, stressing that birth parents and adoptees involved in adoptions that occurred prior to the final passing of this retroactive law be given the right to, if desired, file a disclosure veto to prevent the opening of their sealed files. After being struck down as unconstitutional by the Ontario Superior Court, the *Act* is amended to include Commissioner Cavoukian's proposed disclosure veto.

IPC receives Privacy Innovation Award for work in health

The IPC is presented with the Privacy Innovation Award by the International Association of Privacy Professionals and Hewlett-Packard for its innovative work, including the development of short, easy-to-understand notices to the public about the new health information privacy law.

Commissioner Cavoukian issues first health order under *PHIPA*

Following an investigation by the Commissioner into an incident where personal health records were strewn across Toronto streets as a backdrop to a film production, HO-001 is issued, establishing new standards for the secure destruction of personal information. (The records found on the street were to have been destroyed by a shredding company but were inadvertently sold by its recycling arm as scrap paper to the film company).

2007

Commissioner Cavoukian is named one of the Top 100 Most Powerful Women in Canada

Commissioner Cavoukian is honoured by the Women's Executive Network naming her as one of Canada's most powerful women in the "Trailblazers and Trendsetters" category for her groundbreaking work in protecting privacy.

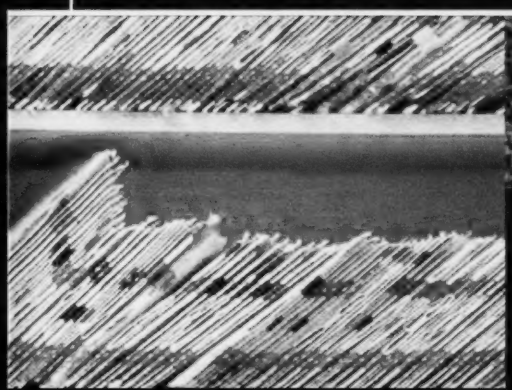
IBM salutes Dr. Ann Cavoukian, Ontario's Information & Privacy Commissioner, on being named one of Canada's Most Powerful Women: Top 100™.

Your unfailing commitment to privacy, and the passion, expertise and energy you devote to privacy issues serve as an inspiration to us all!

IBM

First paper on Biometric Encryption is released

Commissioner Cavoukian launches *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy*, the IPC's first paper on biometric encryption, demonstrating biometrics can be deployed in a privacy-enhanced way that minimizes the potential for surveillance and abuse, maximizes individual control, and ensures full functionality of the systems in which biometrics are used.



The *Personal Health Information Protection Act* (*PHIPA*) comes into force

PHIPA comes into force on November 1, 2004, after substantial input from the IPC. The law governs the manner in which personal health information may be collected, used, and disclosed within the health-care system. It also regulates individuals and organizations that receive personal health information directly from health information custodians. Further, *PHIPA* sets out in law a patient's right to access his or her own medical records, with very limited exceptions.

2006

Divisional Court affirms that the Commissioner has the authority to investigate and report on privacy complaints made by the public against government institutions

In addition, the Court holds that the Commissioner's privacy rulings are protected by "Parliamentary privilege," and are not subject to judicial review by the Courts because they fall within the general oversight and reporting mandate of the Commissioner – as an Officer of the Legislature.

Universities are placed under the *Freedom of Information and Protection of Privacy Act*

As repeatedly advocated by Commissioner Cavoukian, universities and colleges are brought under *FIPPA* on June 10, 2006.

Privacy and Data Protection Commissioners around the world accept the Global Privacy Standard

International Privacy and Data Protection Commissioners accept the Global Privacy Standard (GPS) that a committee of international commissioners, chaired by Commissioner Cavoukian, developed and brought forward. The GPS represents a harmonization of fair information practices into a single instrument, and for the first time, includes the explicit language of data minimization.

2010

Commissioner Cavoukian encourages the health sector to Stop. Think. Protect.

The IPC launches a campaign that calls on leaders in Ontario's health sector to help combat the flow of avoidable breaches involving personal health information. Specifically, health groups are asked to educate members on the simple steps required to prevent the far too frequent disclosure of unencrypted data through the loss or theft of portable electronic devices.

***Access by Design* calls on public institutions to be proactive in releasing information**

Commissioner Cavoukian unveils her concept of *Access by Design*, which consists of 7 Fundamental Principles that encourage public institutions to take a proactive approach to releasing information, making the disclosure of government-held information an automatic process wherever possible – access as the default.

***Privacy by Design* is adopted as an international standard**

A resolution is unanimously passed — by the entire assembly of global Privacy Regulators — recognizing *Privacy by Design* as an essential component of fundamental privacy protection, transforming it overnight into an international standard.

2009

Commissioner Cavoukian is reappointed to an unprecedented third term

Commissioner Ann Cavoukian is reappointed to her third term as Information and Privacy Commissioner of Ontario. The Commissioner states that she will focus her third term on *Privacy by Design*, a concept she first developed in the 1990s to enlist the support of technology to protect privacy, rather than encroach upon it.

The 7 Foundational Principles of *Privacy by Design* launched

Commissioner Cavoukian continues to advance *Privacy by Design* on the world stage with the launch of The 7 Foundational Principles of *Privacy by Design*, which later becomes available in 30 languages.

Commissioner Cavoukian orders Crown attorneys to stop collecting personal information on prospective jurors

Following an extensive investigation, Commissioner Cavoukian orders Crown attorneys to cease collecting any personal information of potential jurors beyond that which is necessary under the *Juries Act* and *Criminal Code*, and proposes a fundamental shift in the way that prospective jurors are screened. The new process addresses the lack of consistency in the "patchwork of practices" employed by Crown attorney offices and the police.

2008

Inaugural *Privacy by Design* Challenge held with support from IBM, Intel, Microsoft, HP and Sun Microsystems

This conference focuses on the emergence and growth of privacy-enhancing technologies (PETs), which Commissioner Cavoukian believes will pave the way for ensuring the future of privacy.

Commissioner engages public discussion on enhanced drivers' licences (EDL)

Commissioner Cavoukian and Professor Andrew Clement hold a public forum on proposed Enhanced Drivers' Licences to provide clear factual information on the voluntary EDL initiative proposed by the government as an alternative to having a passport to cross the U.S. border.

Commissioner Cavoukian releases *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report*

In this report, the Commissioner finds that the Toronto Transit Commission's use of video surveillance is in compliance with Ontario's privacy law, and makes a number of specific recommendations on how privacy can be enhanced.

2011

Year of the Engineer

Commissioner Cavoukian declares 2011 the Year of the Engineer, and challenges those who design and build systems and technology upon which we rely to operationalize *Privacy by Design*.

Commissioner Cavoukian receives international privacy award

Commissioner Cavoukian becomes the first Canadian to receive the 2011 Kristian Beckman Award, which is granted annually to an individual who has "significantly contributed to the development of information security, especially achievements with an international perspective."

Ontario Lottery and Gaming Corporation's (OLG) voluntary self-exclusion program is launched

A partnership between Commissioner Cavoukian, the OLG, and the University of Toronto embeds a design protocol based on *Privacy by Design*, that enables the OLG to better support its customers who have enrolled in a completely voluntary self-exclusion program, while protecting the personal data of all OLG customers.

Top 11 Movers and Shakers in the Global Smart Grid Industry

Intelligent Utility magazine names Commissioner Cavoukian one of the "Top 11 Movers and Shakers in the Global Smart Grid Industry for 2011" for advocating a *Privacy by Design* approach to protecting utility customer data privacy while the Smart Grid is in its infancy.

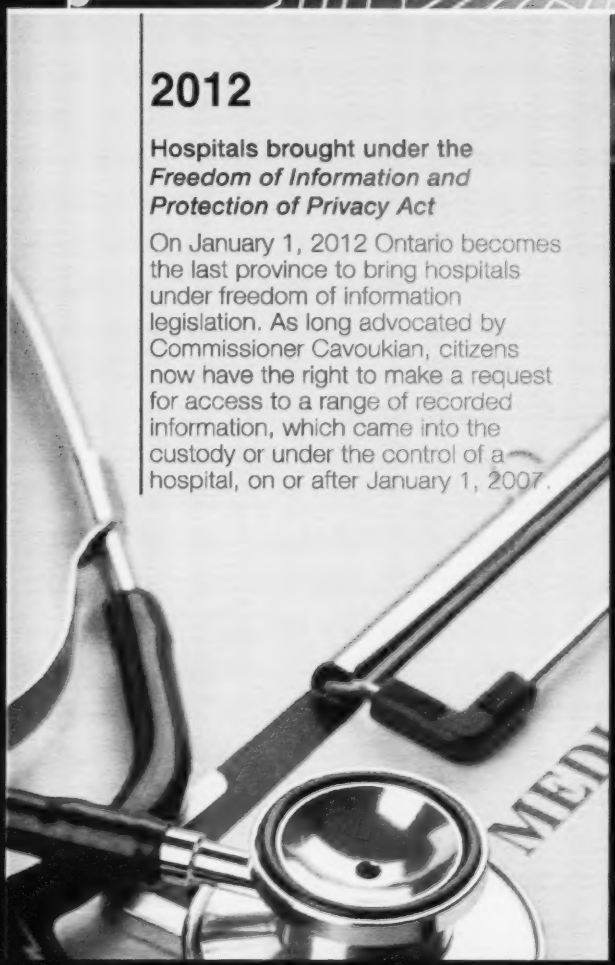
Commissioner Cavoukian named as one of the Top 25 Women of Influence

Women of Influence names Commissioner Cavoukian as one of the honorees in their first annual Top 25 Women of Influence for her groundbreaking work in protecting privacy.

2012

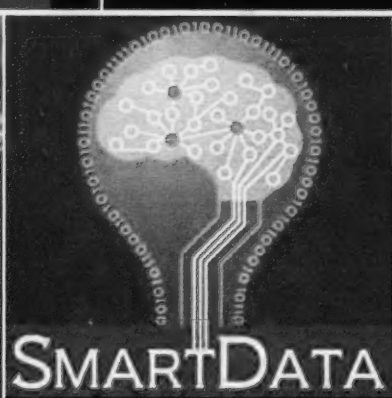
Hospitals brought under the *Freedom of Information and Protection of Privacy Act*

On January 1, 2012 Ontario becomes the last province to bring hospitals under freedom of information legislation. As long advocated by Commissioner Cavoukian, citizens now have the right to make a request for access to a range of recorded information, which came into the custody or under the control of a hospital, on or after January 1, 2007.



Commissioner engages the public on proposed "lawful access" legislation

In response to her grave concerns about impending federal "lawful access" legislation, Commissioner Cavoukian brings together highly-respected thought leaders for a public symposium, *Beware of "Surveillance by Design:" Standing up for Freedom and Privacy*, to raise awareness of the serious implications to the privacy rights of Ontarians, and all Canadians.



The IPC co-presents first International Symposium on SmartData

The Identity, Privacy, and Security Institute, in association with the IPC, brings together world-renowned international and local experts from a wide range of disciplines to discuss the emerging concept of SmartData – a vision to create Internet-based virtual agents, which would act as an individual's online proxy to securely store their personal information and disclose it based upon the context of the data request and instructions of the data subject.

Ontario's Information and Privacy Commissioners: Honourable Sidney B. Linden (1987 – 1991), Dr. Ann Cavoukian (1997-Present), Tom Wright (1991 – 1997)

Commissioner Cavoukian finds that systemic failures at Elections Ontario led to Ontario's largest privacy breach

Over the course of an investigation into Elections Ontario's loss of two USB keys containing the unencrypted personal information of as many as 2.4 million voters, Commissioner Cavoukian finds that the cause can be traced back to the agency's failure to systemically address privacy and security issues. The Commissioner recommends that Elections Ontario take concrete steps in three areas to enhance the protection of personal information – policies, practices, and procedures; training and compliance; and accountability. As a companion to her report, the Commissioner releases a guidance document, *A Policy is Not Enough: It Must be Reflected in Concrete Practices*. This document demonstrates how to effectively execute an appropriate privacy policy and embed it in the concrete practices of an organization.

AbD

Access by Design

First *Access by Design* Ambassadors Appointed

During "Right to Know Week," Commissioner Cavoukian announces the launch of the *Access by Design* Ambassador program, which recognizes thought leaders committed to insuring open and transparent access to government-held information by following The 7 Fundamental Principles of *Access by Design*.

Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices

In order to guide organizations through the implementation of *Privacy by Design*, Commissioner Cavoukian releases a new paper, *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices*. The guide includes an anthology of the experiences of organizations from a wide range of sectors including telecommunications, technology, health care, transportation, and energy. It provides a comprehensive overview of the partnerships and joint projects that the Commissioner has engaged in to implement *Privacy by Design* by outlining concrete and meaningful operational effects to its principles.

NEVER BEFORE IN OUR HISTORY HAS INFORMATION BEEN SO READILY AVAILABLE

Key Issues for 2012

ELECTIONS ONTARIO INVESTIGATION AND REPORT

One of the fundamental rights in a democratic society is the right to vote. Those who choose to exercise their right to vote do so because they have faith in the electoral process. Elections Ontario is entrusted with the responsibility to protect the integrity of the electoral process, including the privacy and security of the personal information of eligible voters.

That is why I was deeply disturbed when Greg Essensa, the Chief Electoral Officer, advised me that staff at Elections Ontario had lost two USB keys containing the unencrypted personal information of between 1.4 million and 2.4 million Ontarians, including full names, home addresses, dates of birth, gender, and whether or not an individual elector had voted in the last provincial election. When Mr. Essensa asked for my assistance in investigating this matter and to advise him on how to prevent another breach from occurring, I, of course, agreed. We received the full cooperation of Mr. Essensa and everyone at Elections Ontario over the course of our investigation.

Ultimately, at the root of the problems uncovered during my investigation was a failure to build privacy into the routine information management practices of the organization. What is particularly discouraging was the discovery that the privacy and security of personal information was not a part of the training programs that were offered to staff – despite the nature of the information in the custody and control of Elections Ontario. The need to protect the privacy and security of elector information entrusted to Elections Ontario must become part of the organizational culture.

To assist them in achieving this imperative, I recommended concrete steps that Elections Ontario must take in three areas to enhance the protection of personal information and restore the trust of Ontarians.

First, Elections Ontario was directed to retain the services of an independent third party to audit the agency's current policies and procedures, as well as to develop an agency-wide privacy policy, including the requirement for any personal information stored on mobile devices to be encrypted.

Secondly, and most important – once developed, privacy policies must be translated into practices and procedures to be effective. This is absolutely essential – the best privacy policies in the world are rendered meaningless if they do not translate into concrete actions taken by staff – the policy must actually be embedded into one's operations.

Thirdly, there must be responsibility and accountability at the highest levels for privacy and security. I recommended that Elections Ontario appoint a Chief Privacy Officer to fill this important role. Also, the Technology Services department should take full responsibility and be totally accountable for training and supporting staff to ensure the implementation of measures to protect the personal information stored on all electronic devices.

I am pleased to report that Mr. Essensa accepted my recommendations unreservedly, and Elections Ontario has made significant progress in implementing them – including the appointment of a Chief Privacy Officer. I remain committed to continue working with the Chief Electoral Officer to ensure that the privacy of Ontario voters is embedded into the agency's operations.

A POLICY IS NOT ENOUGH

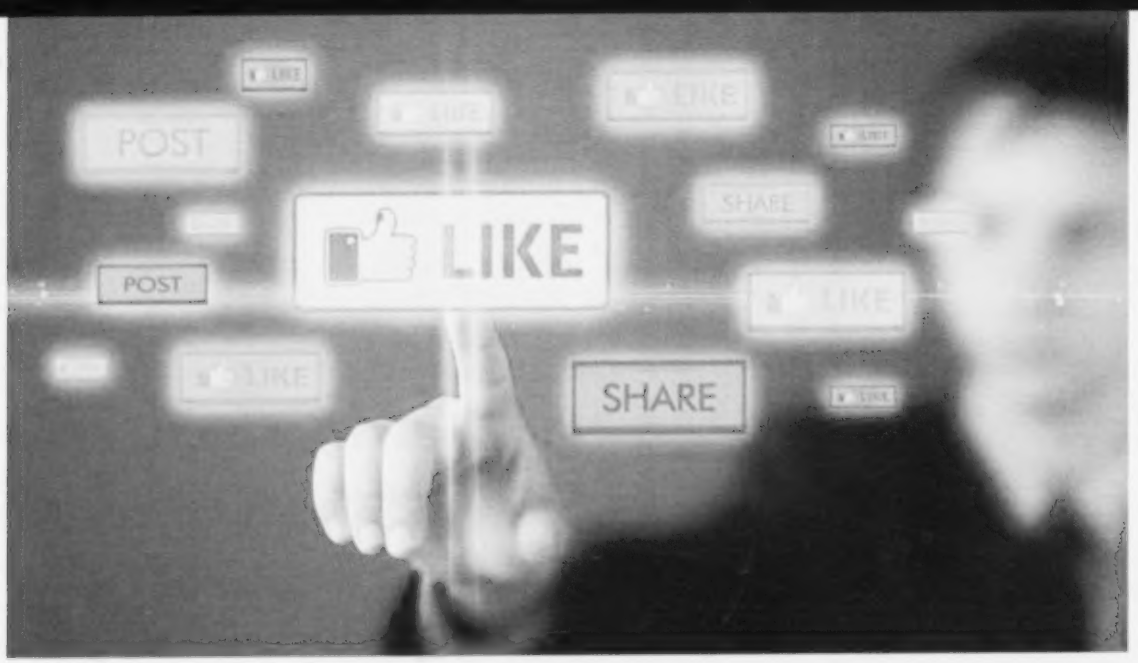
Having a privacy policy cannot, by itself, protect personal information held by an organization. That is why I have produced a new discussion paper, *A Policy is Not Enough: It Must be Reflected in Concrete Practices*, a guide, in effect, which outlines a proactive *Privacy by Design* approach to reducing the risk of privacy harm arising in the first place, while preserving a commitment to functionality. *Privacy by Design*'s flexible, innovation-driven approach to achieving privacy can help to encourage organizations to both internalize the goal of privacy protection and seek out ways to achieve it.

The seven-step action plan outlined in the paper can be used by organizations of any size, and from any sector, as practical guidance for effectively translating their privacy policies into privacy practices. Integrating compliance audits and informal reviews into an organization's procedures will preemptively detect any new privacy challenges, and enable the updating of policies and procedures to deal with issues before a privacy breach occurs.

It is also important to develop education programs that begin with an orientation and remain current through ongoing training. Employees must learn about limitations placed on access to, and use of, personal information, and they need to know about the procedures to be followed if someone makes a request for personal information held by the organization. As well, each organization should designate a knowledgeable "go-to" person who can handle privacy-related questions and concerns.

Despite your best-laid plans, there is still a chance that a breach will occur, and it is important to plan for this by ensuring you have a data breach protocol in place. This would allow you to act both quickly and effectively to meet the expectations of the public, consumers and regulators, and to preserve your organization's reputation.

The most important point I want you to take away is that a policy is not enough – you have to put it into practice! This means you have to communicate it, educate your staff, and have measures in place to ensure that the policy doesn't just sit on a shelf somewhere, but is translated into concrete actions.



KEEP IT PRIVATE!

Engaging in social media can be a very enjoyable pastime, but people's perceptions of their privacy fall far short of reality, and they lack awareness of the potential ramifications. Despite their many positive aspects, the lack of awareness regarding the privacy and confidentiality of sensitive information is a major drawback to social networking sites. Anything associated with you, or the people you are connected to, will most likely be viewed and evaluated by other people, some of whom may have considerable influence over your life, now or well into the future. If employment decisions about you were made based on information obtained from social networking websites, you may never know why you didn't get the job, the interview, or the promotion.

Early in 2012 there were numerous recent media reports of employers in the United States requesting Facebook passwords from job candidates or asking job applicants to "friend" a human resources staff member so the employer may review their online activities. Some employers have gone so far as to ask candidates to provide them with their username and password. This intrusive practice has put many people in the difficult position of having to choose between obtaining employment or disclosing their usernames, passwords and the intimate details of their lives.

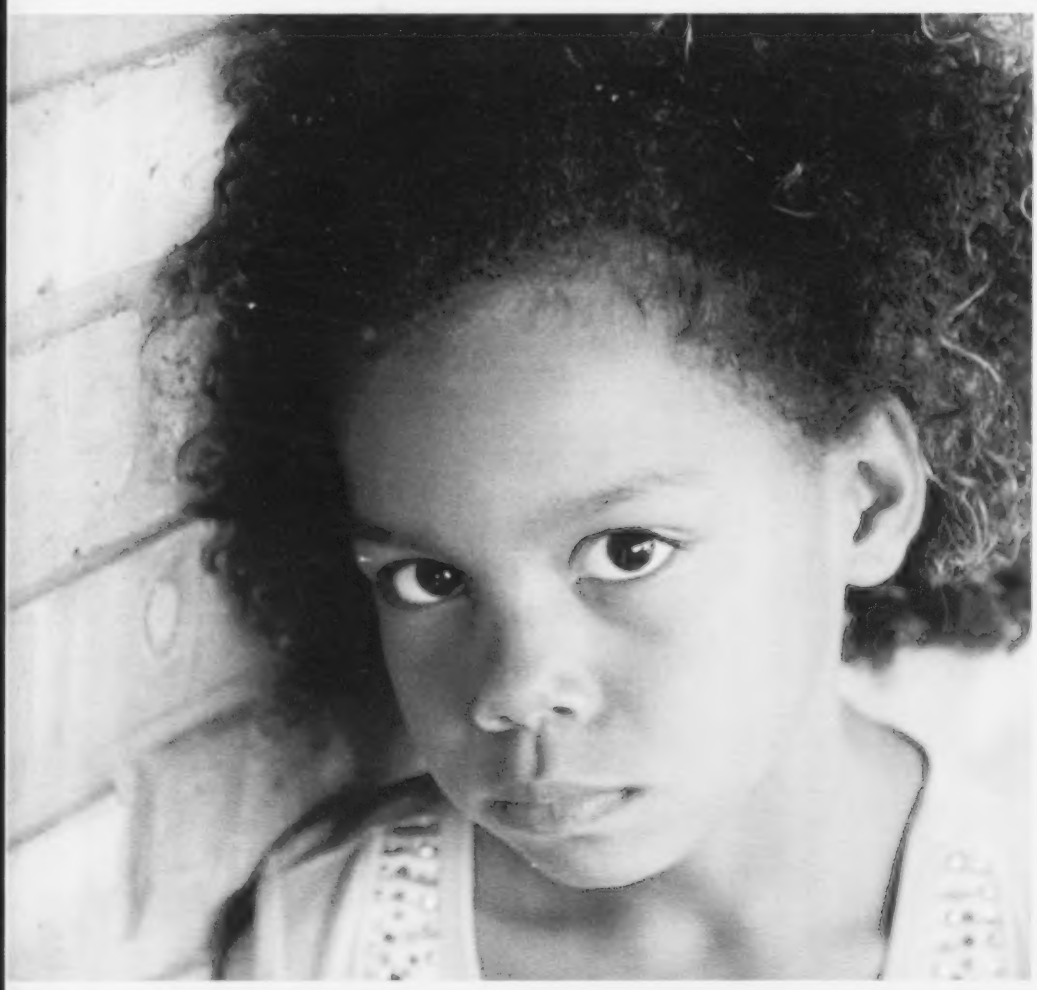
Fortunately, this does not appear to be the case in Canada, where human rights and privacy laws provide stronger protections for job applicants. Employers cannot ask for information that may directly or indirectly reveal a prohibited ground of discrimination. In Ontario, requests for this kind of information may also put the employer at risk of a lawsuit as an unreasonable intrusion into not only an applicant's private activities, but also the activities of their "friends."

To provide Ontarians with practical advice to protect personal privacy in today's constantly-evolving online world, I released a new paper, *Reference Check: Is Your Boss Watching? The New World of Social Media: Privacy and Your Facebook Profile*, which offers true-to-life examples of improper practices by employers, and most importantly, offers practical tips to protect personal privacy.

STOP BULLYING ... BY DESIGN

Social media networks like Facebook and Twitter appear to have become the new schoolyard for bullies. But unlike the tormentors of the playground, cyberbullies are able to lurk in the shadows of anonymity on the Internet, and their cruelty doesn't stop at the end of the school day. The harm they inflict on their victims can have devastating effects, and too often leads to the most tragic of consequences.

Following the death of Amanda Todd, I was compelled to add my voice to the growing chorus of those opposing bullying and released a video blog on the subject. I also reached out to junior high school students, presenting to them about actual incidences of bullying and its heartbreaking consequences and what to do if they found themselves being victimized. I called on those who witness bullying to get involved and speak up – bullies pick on individuals, not groups! They can also demonstrate the real way to be popular, by supporting victims of bullying by offering them help and support – letting them know they are not alone.



In the fall I launched a new initiative, *Stop Bullying... by Design*. The first phase was the creation of a new section on my website with information about online safety, what to do if you become the victim of a bully, or if you witness a bullying incident, advice for parents and teachers, and important resources.

In 2013 I will continue to speak out against the bullying and draw attention to its devastating consequences as well as expand the *Stop Bullying... by Design* initiative. Stay tuned for more details!

DEMONSTRATING INNOVATION AND LEADERSHIP IN THE FIELDS OF BOTH ACCESS AND PRIVACY

2012 Statistics

IN 2012,
ONTARIO HOSPITALS WERE
BROUGHT UNDER THE
FREEDOM OF INFORMATION
AND PROTECTION
OF PRIVACY ACT
A HISTORICAL
EVOLUTION
MILESTONE
OF FREEDOM OF INFORMATION

HIGHLIGHTS
FOR 2012
937 FREEDOM OF INFORMATION
REQUESTS
WERE SUBMITTED TO
ONTARIO HOSPITALS
845 REQUESTS
WERE COMPLETED, WITH AN EXTENDED
COMPLIANCE RATE OF 95 PER CENT

ACCESS

Broader Public Sector Accountability Act came into effect

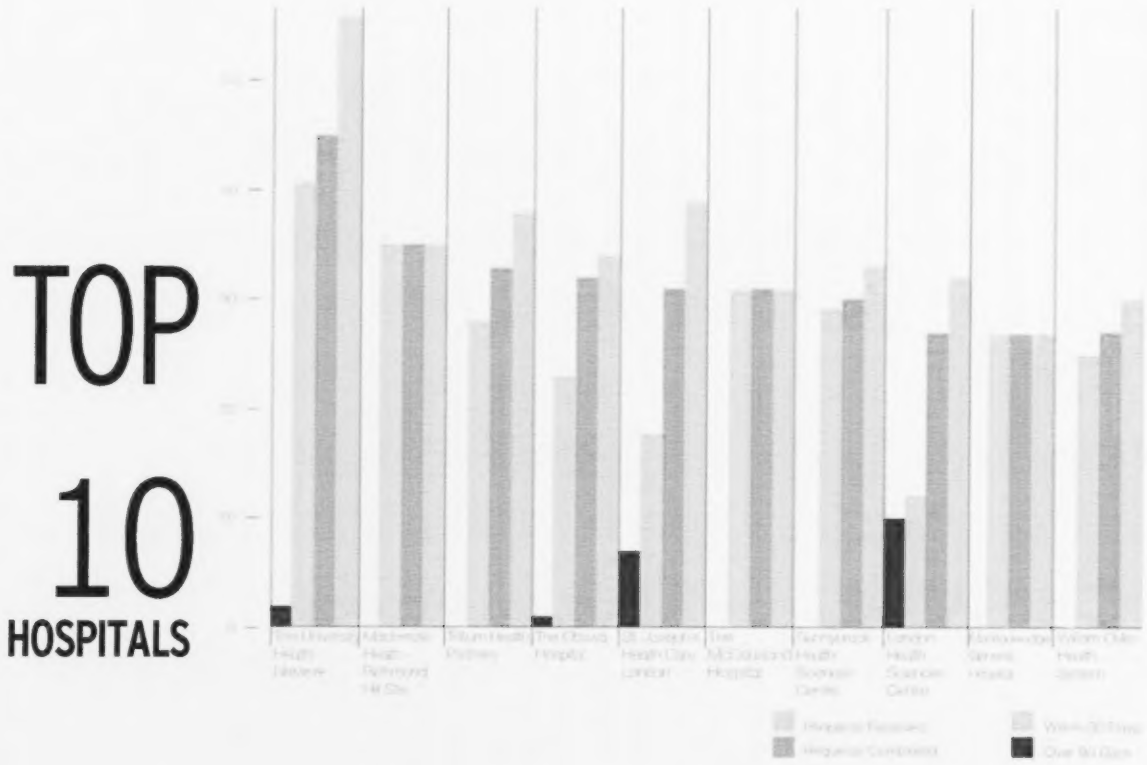
On January 1, 2012, the *Broader Public Sector Accountability Act* took effect, bringing Ontario's hospitals under the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) – a historical milestone in the evolution of freedom of information in Ontario. To support hospitals in implementing this new legislation, I dedicated much of the year to working with stakeholders such as the Ontario Hospital Association, giving presentations, producing video messages and participating in outreach initiatives.

By all accounts, the first year appears to have gone well, but as anticipated, when the first FOI requests were filed some hospitals had questions. My office fielded many calls asking for information about the application of *FIPPA* within the context of their operations and we continued to distribute our key guidance documents, *Applying PHIPA and FIPPA to Personal Health Information: Guidance for Hospitals* and *Freedom of Information at Ontario Hospitals: Frequently Asked Questions*.

Starting this year, hospitals in Ontario must complete and provide my office with reports that discuss the hospital's activities under both the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) and the *Personal Health Information Protection Act* (*PHIPA*). To help prepare them for filing their statistics we held a joint educational webinar with the Ontario Hospital Association entitled, *FIPPA and PHIPA Annual Statistical Reporting Requirements to the Information and Privacy Commissioner of Ontario*.

Working with Ontario's hospitals has been a major endeavour for my staff, but one that is well worth it. I believe we were successful in reassuring hospitals and their staff that the new legislation would not interfere with

Open Data, Big Data, Yes... Personal Data, No! at the Toronto Board of Trade. Samantha Liscio, Corporate Chief Strategist, Ministry of Government Services; Daphne Gaby Donaldson, Executive Director, Corporate Information Management Services, City of Toronto; Dave Wallace, Chief Information Officer, University of Waterloo; Jury Konga, Principal, eGovFutures Group; Brian Beamish, Assistant Commissioner, Information and Privacy Commissioner, Ontario; Dr. Ann Cavoukian, Information and Privacy Commissioner, Ontario



the delivery of health care but would provide another layer of legitimacy in making our public institutions more transparent and accountable.

Open Data Event

Without access to information held by government institutions, citizens cannot participate meaningfully in the democratic process and hold government accountable to the people it serves. Unless there is sufficient reason to the contrary, government-held information should be free and easily accessible – by default.

In September, my office hosted an event on the global Open Data movement with the Toronto Board of Trade to mark Right to Know Week 2012, which is celebrated by freedom of information organizations in over 40 countries around the world. I called on public institutions in Ontario to take advantage of emerging technologies to make data available to the public, academics, researchers, and industry, for use in new and unanticipated ways. I believe that the goals of openness and privacy can be achieved by embracing Open Data as demonstrated very effectively by municipalities in Ontario such as the City of Toronto. Open Data, when implemented properly, will improve service delivery, increase transparency, and raise levels of accountability and citizen trust in government, while strongly protecting privacy.

I was heartened to learn that the Ontario Public Service is embracing my concept of *Access by Design* (*AbD*) as part of the long-range plan for Ontario's Open Data portal. This to me only makes sense since Open Data is one of the truest embodiments of *AbD*, by which public institutions proactively release information as part of an automatic process, fostering more transparency and

accountability in government. Soon after the event, the government of Ontario took the first steps in launching its own Open Data portal. I am looking forward to seeing Ontario's Open Data site grow by leaps and bounds in 2013.

Access by Design Ambassador Program

After my concept of *Privacy by Design* started gaining ground around the world, I was confident that the same kind of positive-sum paradigm could be applied to freedom of information and the concept of *Access by Design* (*AbD*) was born. I developed the *7 Fundamental Principles of AbD* because I wanted to address the way that government and citizens interacted and to encourage public institutions to take a proactive approach to releasing information, making the disclosure of government-held information an automatic process where possible – access as the default.

The principles of *AbD* may be applied to almost all types of non-personal government-held information, but the emphasis is on information that allows citizens to hold their government accountable. When information is freely available, the public may question the actions of their government and participate meaningfully in policy decisions. Government transparency and access to information are vital ingredients for a free and functioning democratic society. Citizens must be provided the right to government-held information in order to participate meaningfully in civil life – something which is not possible if government activities are hidden from public view. Additionally, *AbD* goes much further than just routine disclosure – it calls for a more responsive and efficient government that forges collaborative relationships with citizens, the private sector, and other public institutions.

In that spirit, I also wanted to reach out and forge collaborative relationships with respect to *AbD*, which is why I created the *Access by Design (AbD)* Ambassador program. Whenever an individual or organization is brought to my attention that promotes access to information, Open Data or applies the principles of *AbD*, they are invited to join the *AbD Ambassador* program. Since September, we have inaugurated five *AbD* Ambassadors and I am hoping to induct many more in 2013. If you believe you know of an individual or organization that deserves to be inaugurated as an *AbD* Ambassador, please contact my office. We are always looking for allies in the campaign for access to information.

Highlights from 2012 Orders

PO-3009 University of Ottawa

An appellant made a request to the University of Ottawa under the *Freedom of Information and Protection of Privacy Act* (*FIPPA*), for records that mentioned his name, some of which were in the possession of professors who were members of the Association of Professors of the University of Ottawa (APUO). The university asked APUO members to turn over the records so that it could make an access decision under the *Act* from which APUO filed a grievance. The IPC's adjudicator set out the principles that should be applied in determining whether records in the possession of faculty members are within the custody or control of a university for the purposes of *FIPPA*. The adjudicator also clarified that the issue of custody or control is properly within the purview of the IPC, not the grievance process.

PO-3050 Carleton University

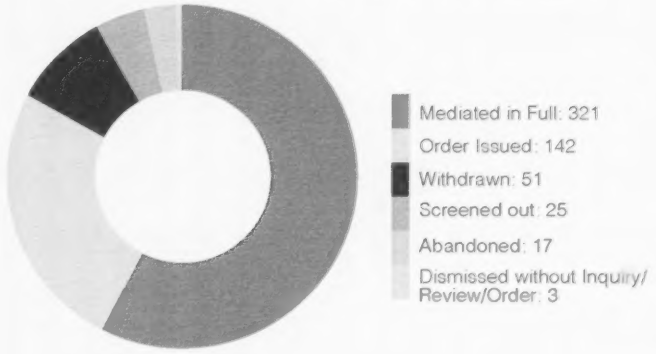
An appellant questioned a search performed by Carleton University after a request was made for records, including deleted emails, held by the university's Department of Law. The university took the position that emails deleted by a particular professor were beyond the scope of the appellant's request. The IPC found that in the unique circumstances of this case, the deleted emails were within the scope of the appellant's request and that, as a result, an adequate search for responsive records had not been performed. However, the IPC's adjudicator went on to state that a request for emails does not normally encompass a search for deleted emails.

PO-3084 University of Ottawa

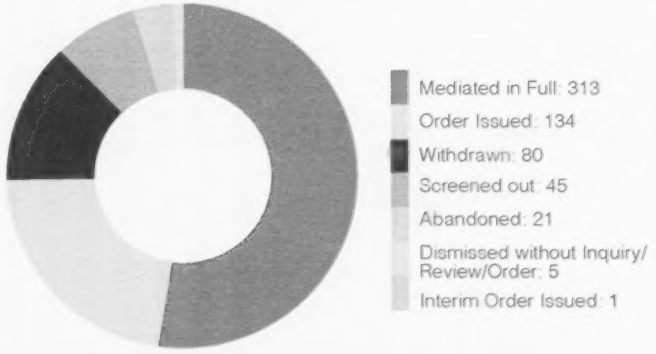
An appellant made a request to the University of Ottawa for all expense reports related to research projects submitted by two named professors. The university identified records responsive to the request and issued a decision advising that, pursuant to section 65(8.1), the *Act* did not apply to the requested records as they were associated with research. This Order found that Section 65(8.1) did in fact apply to the records at issue and the university's decision was upheld.

APPEAL OUTCOME

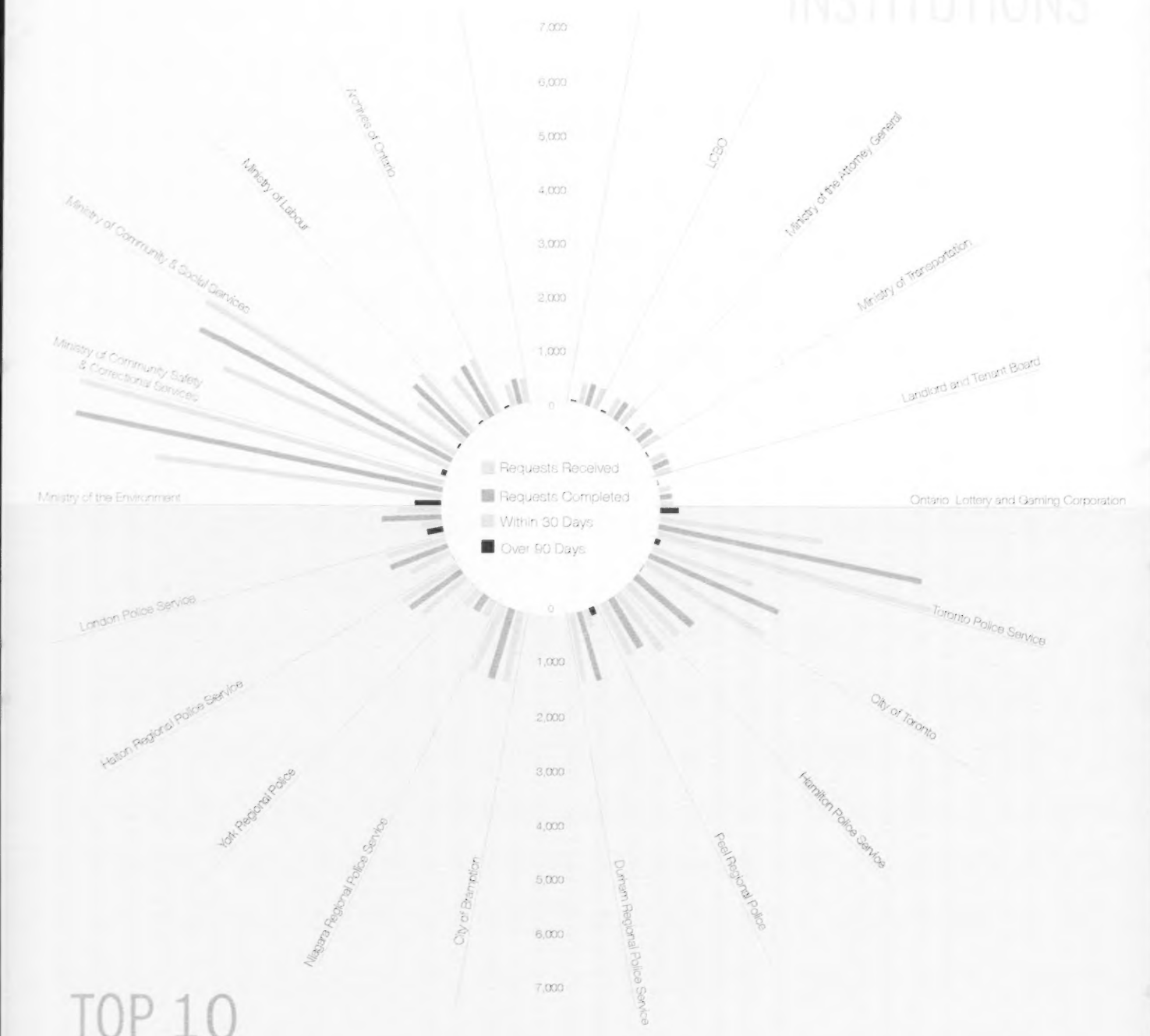
PROVINCIAL



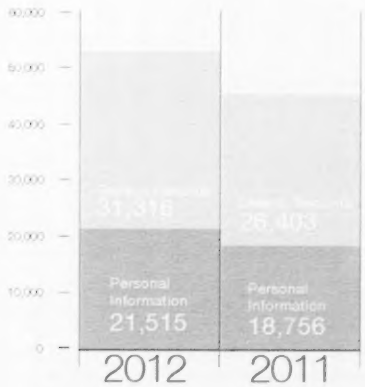
MUNICIPAL



TOP 10 PROVINCIAL INSTITUTIONS



TOP 10 MUNICIPAL INSTITUTIONS



OVERALL REQUESTS

↑15 Personal Information

↑19 General Records

↑17 Total Requests

2012 AT A GLANCE

PROVINCIAL SUMMARY

PERSONAL INFORMATION

REQUESTS
2012 5,813 ↑11%
2011 5,237

APPEALS OPENED
2012 163 ↑ 6%
2011 154

APPEALS CLOSED
2012 164 ↑13%
2011 146

AVERAGE COST
2012 $4.98 ↓56%
2011 $11.26

GENERAL RECORDS

REQUESTS
2012 14,158 ↑19%
2011 11,918

APPEALS OPENED
2012 456 ↓ 3%
2011 469

APPEALS CLOSED
2012 395 ↑17%
2011 337

AVERAGE COST
2012 $41.99 ↑ 1%
2011 $41.39

TOTAL REQUESTS
2012 19,971 ↑16%
2011 17,155

PRIVACY COMPLAINTS OPENED
2012 155 ↑18%
2011 131

PRIVACY COMPLAINTS CLOSED
2012 154 ↑19%
2011 129

MUNICIPAL SUMMARY

PERSONAL INFORMATION

REQUESTS
2012 15,702 ↑16%
2011 13,535

APPEALS OPENED
2012 265 ↑ 2%
2011 259

APPEALS CLOSED
2012 230 ↓ 6%
2011 246

AVERAGE COST
2012 $9.67 ↑10%
2011 $8.83

GENERAL RECORDS

REQUESTS
2012 17,158 ↑19%
2011 14,466

APPEALS OPENED
2012 392 ↑18%
2011 333

APPEALS CLOSED
2012 369 ↑25%
2011 296

AVERAGE COST
2012 $27.30 ↑13%
2011 $24.22

TOTAL REQUESTS
2012 32,860 ↑17%
2011 28,001

PRIVACY COMPLAINTS OPENED
2012 127 ↓ 6%
2011 135

PRIVACY COMPLAINTS CLOSED
2012 121 ↓18%
2011 148

"WE DO NOT, AND NEVER WILL, ACCEPT THE PROPOSITION THAT THE BUSINESS OF THE PUBLIC IS NONE OF THE PUBLIC'S BUSINESS."

THE HONOURABLE IAN SCOTT,
ATTORNEY GENERAL OF ONTARIO
1985–1990

2012 HIGHLIGHTS

52,831

A new record for freedom of information (FOI) requests filed across Ontario in 2012

17%

Increase over 2011 when 45,159 requests were filed

81.8%

30-day compliance rate for provincial ministries, agencies and institutions

76.7%

30-day compliance rate for municipal government organizations

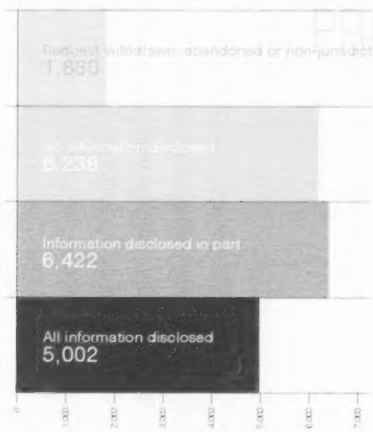
$31.22

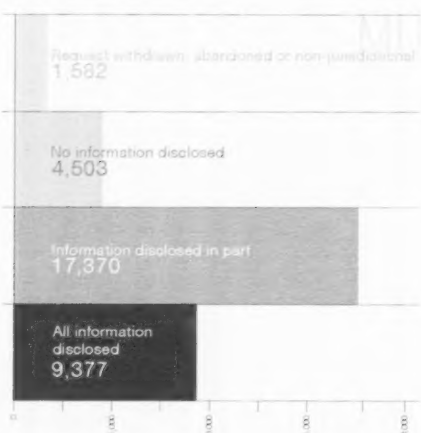
Average fee: provincial

$18.81

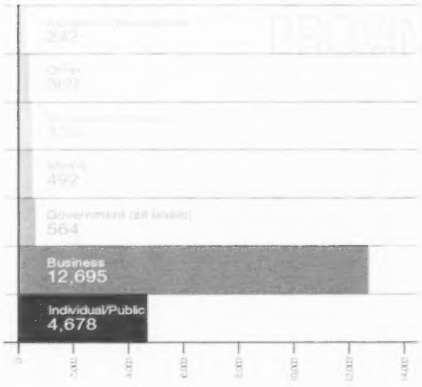
Average fee: municipal

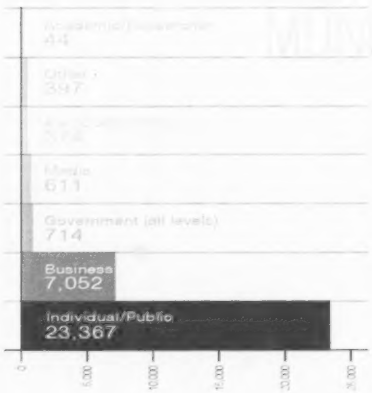
OUTCOME OF REQUESTS



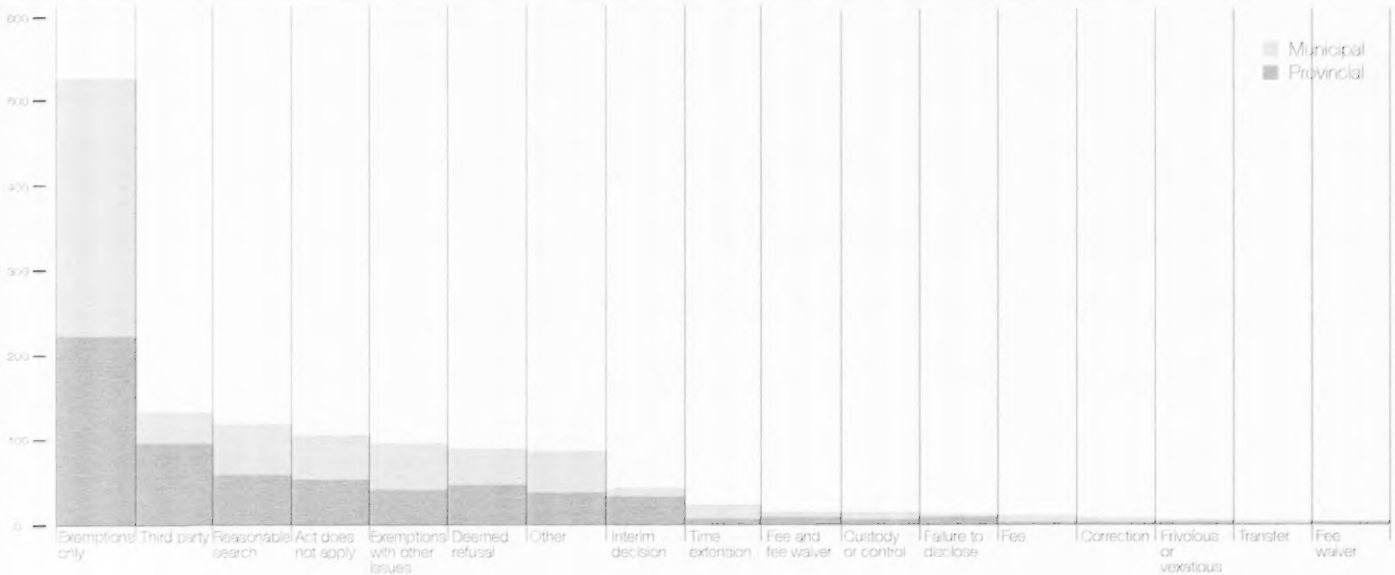


REQUESTS COMPLETED BY SOURCE





ISSUES IN APPEALS OPENED



1,276
Total appeals opened by the IPC in 2012

5%
Increase over 2011

1,158
Total appeals closed by the IPC in 2012

13%
Increase over 2011

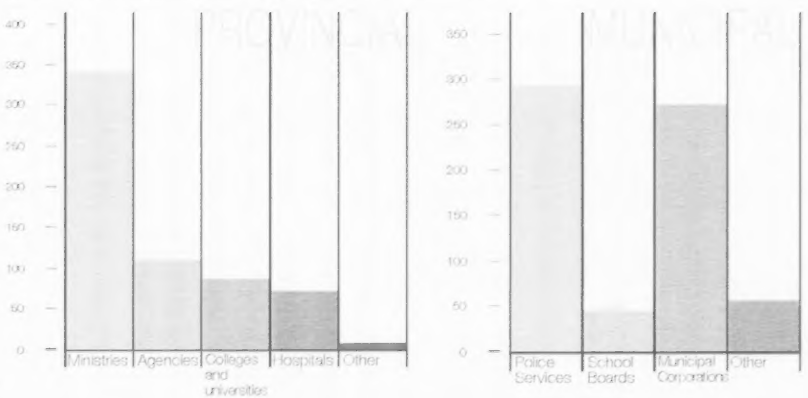
634
Appeals were mediated in full

277
Resulted in an Order

79.1%
Appellants were individuals

14%
Appellants were businesses

APPEALS BY INSTITUTION TYPE



25 YEARS
FREEDOM OF INFORMATION REQUESTS AND PRIVACY COMPLAINTS

651,822

Freedom of Information (FOI) requests received in Ontario

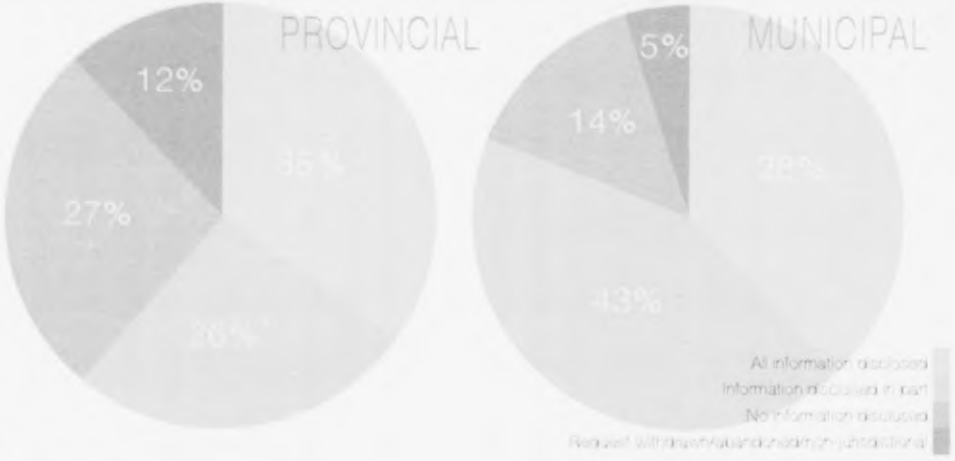
296,140

FOI requests received by provincial ministries, agencies, and institutions

355,682

FOI requests received by municipal government organizations

OUTCOME OF REQUESTS COMPLETED FROM 1988-2012



95% FOI requests completed

274,652 PROVINCIAL

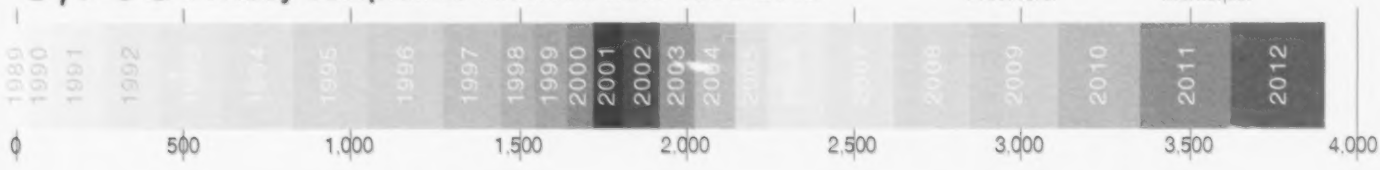
345,824 MUNICIPAL

PRIVACY COMPLAINTS IN ONTARIO OVER 25 YEARS

3,905 **Privacy complaints** received from 1988-2012

2,139 **Total received** Provincial

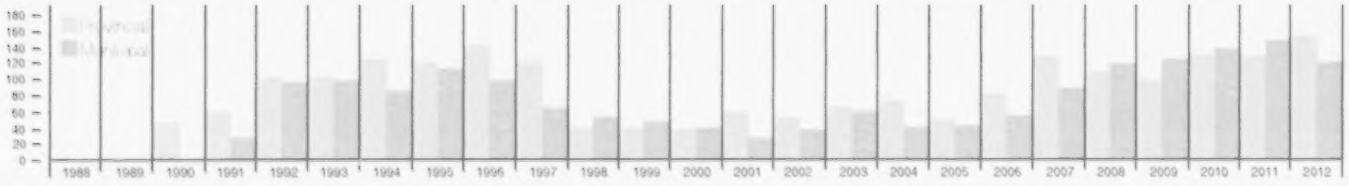
1,766 **Total received** Municipal



3,828 **Privacy complaints** completed since 1988

2,089 **Total completed** Provincial

1,739 **Total completed** Municipal



25 YEAR HIGHLIGHTS

TIME TO COMPLETION OVER 25 YEARS

85%

Highest provincial compliance rate under 30 days was in 2008

91%

Highest municipal compliance rate under 30 days was in 1992 and 1993

190,472

Requests completed by provincial institutions 30 days or less

288,469

Requests completed by municipal institutions 30 days or less

APPEALS 1988 – 2012

23,202

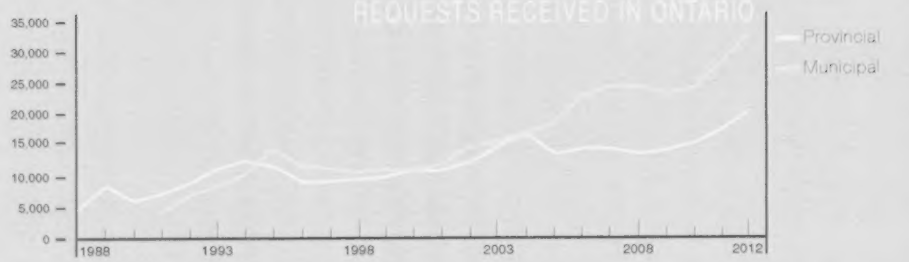
Appeals received by the IPC between 1987 and 2012

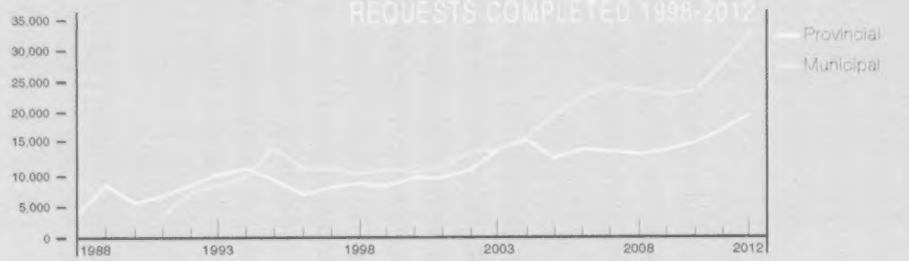
22,170

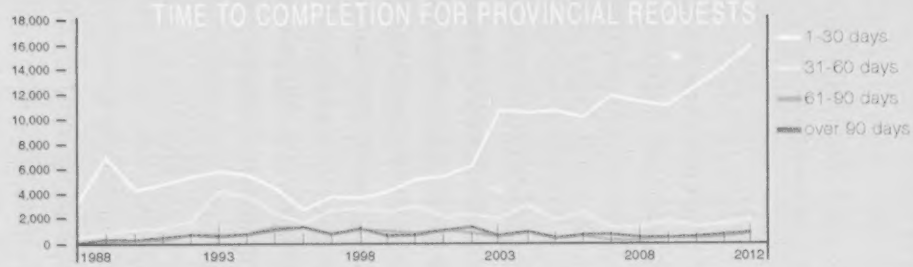
Appeals resolved by the IPC between 1987 and 2012

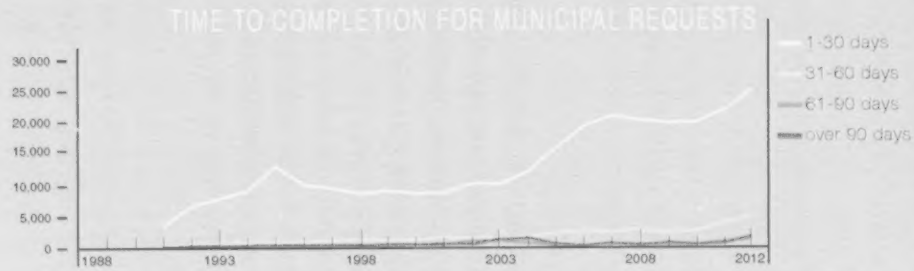
6,235

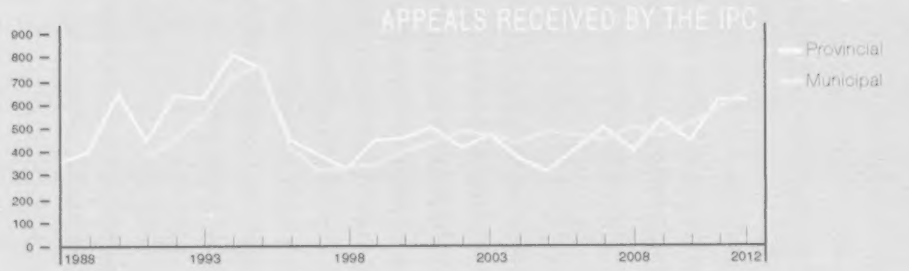
Orders issued for provincial and municipal appeals by the IPC











PHIPA IN 2012

The following are highlights from 2012 that are relevant to the *Personal Health Information Protection Act* (*PHIPA*), which my office has overseen since it was passed in 2004. Personal health information comprises some of the most sensitive and intimate details of one's life. As such, it requires strong protection to ensure the privacy of the individual to whom it relates. Personal health information must also be accurate, complete, and accessible to health-care providers in order to deliver necessary health care to individuals. At the same time, health information has long been used for invaluable secondary purposes that go beyond the care and treatment of the individual, for uses that are seen to benefit society as a whole, such as research and health system planning and evaluation.

This year we undertook the following initiatives to continue to educate the health sector on *PHIPA*:

Embedding Privacy into the Design of Electronic Health Records

Embedding *Privacy by Design* into electronic health record (EHR) systems will enable us to benefit from the wealth of health information stored on these systems, while protecting privacy. By incorporating the principles of *Privacy by Design*, privacy can be protected, or even enhanced, while enabling the use and disclosure of health information to improve the delivery of health care and ensure the effective and efficient operation of our health system.

In February, my office released *Embedding Privacy Into the Design of EHRs to Enable Multiple Functionalities – Win/Win*, which I co-authored with Richard C. Alvarez, President and CEO of Canada Health Infoway. The paper explores how to maximize both the benefits of protecting privacy and the benefits of using and disclosing health information for secondary purposes and outlines some of the components needed to establish a governance framework for such uses and disclosures in the EHR context. One of the main premises of the paper is that, as a general rule, personal health information should be de-identified prior to its use or disclosure for secondary purposes.

Dispelling the Myths under the *Personal Health Information Protection Act*

There are many myths surrounding the duties and obligations imposed by *PHIPA* on health information custodians. My office worked with some key stakeholders in the health sector to identify and dispel the more common myths, including:

- Express consent is required to share personal health information for health-care purposes;

- Express consent must be provided in writing;
- Individuals do not have a right to see or get a copy of their own records;
- Personal health information cannot be used for educational purposes; and
- Personal health information can never be shared with family members

In September, a one-page document *Dispelling the Myths Under the Personal Health Information Protection Act*, was released by my office in conjunction with the Ontario Hospital Association, the Ontario Medical Association, the Canadian Medical Protective Association, the College of Physicians and Surgeons of Ontario, the Ontario Association of Community Care Access Centres and the Ministry of Health and Long-Term Care.

Unauthorized Access to Health Records

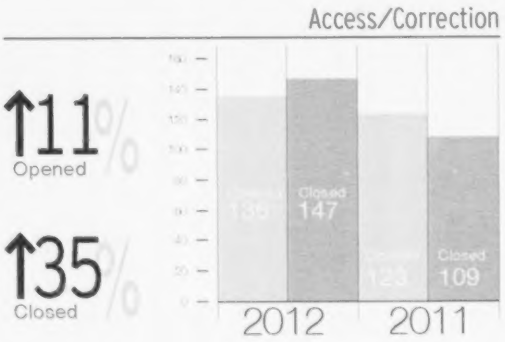
Since the introduction of *PHIPA*, hospitals and other health information custodians have made tremendous strides to ensure that the privacy of personal health information remains a top priority. However, in some instances, privacy breaches have occurred. In a number of instances, personal health information has been accessed by authorized health-care providers for unauthorized purposes. For example, health-care providers not involved in the delivery of health care to an individual have accessed that individual's personal health information for purposes such as curiosity or personal gain.

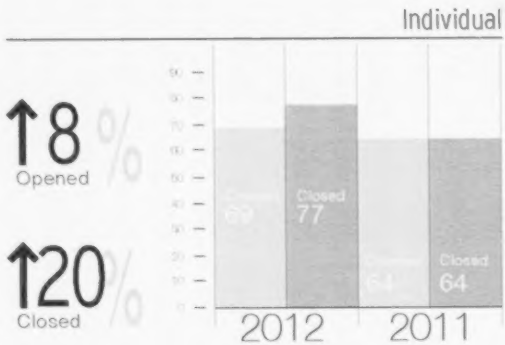
To help hospitals prevent incidents of unauthorized access through education and training, my office collaborated with the Ontario Hospital Association to develop an "Unauthorized Access e-Learning Module" and a primer entitled "Preventing/Reducing Unauthorized Access to Personal Health Information," which were presented in a webcast on November 26, 2012.

This module is an interactive, scenario-based, training tool that explains the purposes for which personal health information may be collected, used and disclosed, outlines the potential consequences of unauthorized access and describes the hospital's role in preventing unauthorized access.

The primer is focused on the steps that the hospital should take to prevent or reduce unauthorized access by setting out best practices for safeguarding personal health information.

As the keynote speaker at the webcast, I reinforced the need to wrap a cloak of privacy around the delivery of health care, to integrate privacy into all programs and services and to ensure all agents are aware of the privacy policies, procedures and practices implemented by the hospital and how to apply them in their daily work.





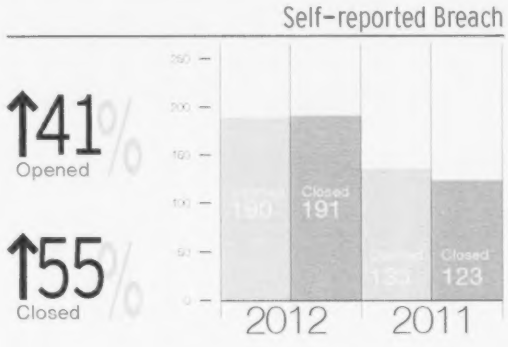
Encryption by Default and "Circles of Trust"

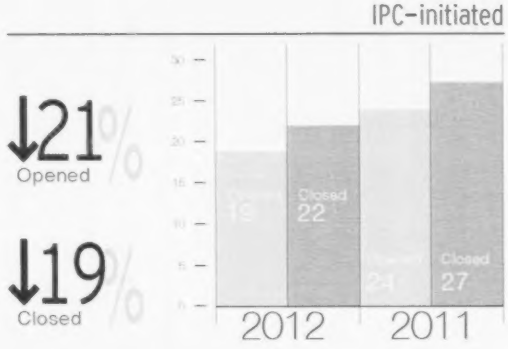
My office partnered with Sunnybrook Health Sciences Centre and CryptoMill Technologies, a security technology solutions company, to co-author a discussion paper examining two of the biggest information security risks faced by health-care organizations – securing personal health information on portable media against theft, loss and unauthorized use or disclosure, and applying effective role-based access controls.

The paper, *Encryption by Default and Circles of Trust: Strategies to Secure Personal Information in High-Availability Environments*, advocates encrypting all personal health information by default and assigning access rights to different user groups called "Circles of Trust". The paper takes as its central challenge the need to mitigate security risks while assuring fast and reliable access to personal health information for health-care purposes.

One approach is to establish technological boundaries within which personal health information may flow freely and be accessible for authorized purposes, but beyond which it is unreadable, by default. The application of "Circles of Trust" is modeled after the concept of the "Circle of Care" which refers to the ability of certain health information custodians to share personal health information under *PHIPA* for the purpose of delivering health care to the individual on the basis of assumed implied consent.

The paper seeks to stimulate discussion of the challenges and opportunities for enhancing the security of personal health information beyond that which is currently in place in health-care settings. The paper examines the challenges of applying organization-wide "encrypt by default" policies in large, complex, and dynamic health-care operating environments. It proposes that health-care organizations can benefit from improvements in privacy and security without significant user or institutional burden, resulting in a positive-sum outcome.





JUDICIAL REVIEWS

In 2012 the Courts continued to give a strong measure of deference to the IPC's decisions engaging the transparency and public accountability purposes of the statutes. In a particularly important case, the Divisional Court affirmed the IPC's decision that the public interest in disclosure of information concerning the expenditure of public funds outweighed personal privacy interests in the salary details of highly paid public servants.

The Regional Municipality of York Police Services Board ("Board") brought an application for judicial review seeking to quash the IPC's Order MO-2563. That decision required the Board to disclose to the York Regional Police Association the base salary amounts paid to the Board's Chief and Deputy Chiefs of Police ("affected parties") for the years 2009-2012. The total salary amounts paid to these individuals substantially exceeded $100,000 in each year and, accordingly, were already disclosed under Ontario's "Sunshine" law, the *Public Sector Salary Disclosure Act* ("*PSSDA*"). The additional disclosure of the base salary amounts taken from their contracts of employment would have the effect of revealing the difference between those amounts and their actual total salaries for the years in question, and would thus reveal the "pay for performance" amounts paid to these individuals which made up the difference.

The IPC found that the base salary amounts comprised the affected parties' "personal information" and disclosed their "income". These amounts were therefore subject to the presumption of an unjustified invasion of privacy at section 14(3)(f) of the *Municipal Freedom of Information and Privacy Act* ("*MFIPPA*") and were exempt from disclosure under the personal privacy exemption at section 14(1). However, the IPC went on to apply the "public interest override" at section 16 and found that there was a compelling public interest in disclosing the components of total compensation paid from the public purse to senior public servants. Further, this public interest outweighed the limited privacy interests of the affected parties in shielding the information in issue. Because the public interest override applied, the base salary information was ordered disclosed.

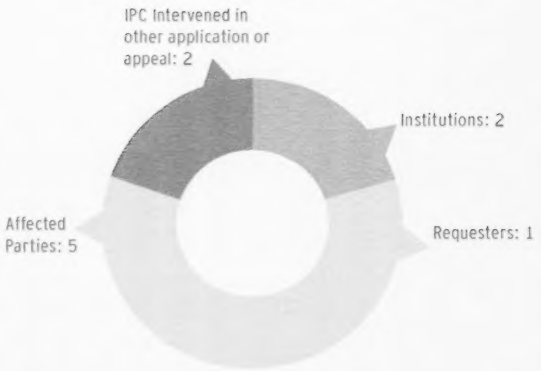
On judicial review the Board argued that IPC's decision was unreasonable because: (1) it failed to balance the privacy interests of the affected persons; (2) there was no compelling interest justifying disclosure; and (3) the *PSSDA*, which the Board submitted was the sole statutory mechanism governing disclosure of the income of public servants, did not require disclosure

of the base salary information. The Court was not persuaded by these arguments and held that the IPC reasonably balanced both access and privacy interests at stake, as evidenced by the following passage from the decision (in part):

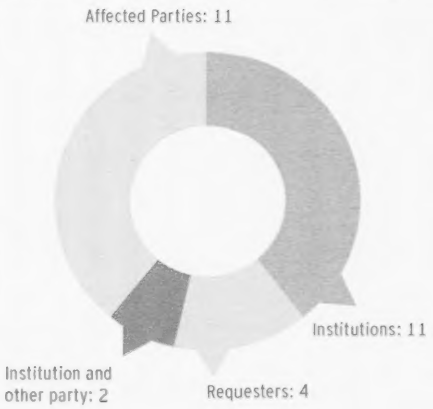
> The public has a right to know to the fullest extent possible how taxpayer dollars have been allocated to public servants' salaries, and this has particular force with respect to public servants at senior levels who earn significant amounts of money paid out of the public purse. Certainly, the *PSSDA* is one important tool for ensuring such openness and transparency. However, in my view, to limit disclosure to only those amounts that are disclosed under the *PSSDA* seems incongruent with the government's commitment to openness and transparency and, in turn, accountability for the allocation of public resources. In my view, when an individual enters the public service he/she accepts that his/her salary may be exposed to public scrutiny. In this case, the amounts at issue exceed the *PSSDA* $100,000 threshold and the impact on the affected parties' privacy is limited ... In my view, the need for complete transparency in this case outweighs the limited privacy interests of the affected parties.

The Court stated that this decision, including interplay between the *PSSDA* and *MFIPPA*, lies at the core of the IPC's mandate and falls well within the range of acceptable outcomes. The Court's ruling is therefore significant in its recognition that the IPC's expertise extends to the interpretation of external legislation which raises issues under her home statutes.

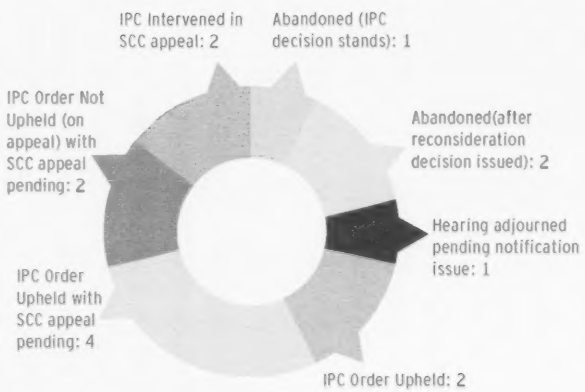
New Judicial Review applications received in 2012



Outstanding Judicial Reviews as of December 31, 2012



Judicial Reviews closed/heard in 2012


IPC Intervened in SCC appeal: 2
Abandoned (IPC decision stands): 1
IPC Order Not Upheld (on appeal) with SCC appeal pending: 2
Abandoned(after reconsideration decision issued): 2
Hearing adjourned pending notification issue: 1
IPC Order Upheld with SCC appeal pending: 4
IPC Order Upheld: 2

FINANCIAL STATEMENT

	2012-2013 Estimates $	2011-2012 Estimates $	2011-2012 Actual $
SALARIES AND WAGES	10,132,000	9,852,800	9,480,694
EMPLOYEE BENEFITS	2,330,900	2,266,600	1,852,489
TRANSPORTATION AND COMMUNICATIONS	337,500	337,500	251,138
SERVICES	1,960,300	2,052,300	1,917,066
SUPPLIES AND EQUIPMENT	336,000	439,000	470,987
TOTAL	15,096,700	14,948,200	13,972,374

Note: The IPC's fiscal year begins April 1 and ends March 31.
The financial statement of the IPC is audited on an annual basis by the Office of the Auditor General of Ontario.

2012 APPEALS FEES DEPOSIT

(Calendar year)

GENERAL INFO.	PERSONAL INFO.	TOTAL
$13,429	$2,780	$16,209

See further financial information, including IPC Public Sector Salary Disclosure, at www.ipc.on.ca

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO
2012 ANNUAL REPORT

2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Canada

Tel: (416) 326-3333
Fax: (416) 325-9195
1-800-387-0073
TTY: (416) 325-9539

E-mail: info@ipc.on.ca
Web: www.ipc.on.ca